NEW YORK STATE SUPREME COURT
NEW YORK COUNTY
----------X

CYNTHIA GARRETT; HENRY GONZALEZ;
SCOTT CHUNG; CURT BURNS; DAVID COOPER;
CRAIG BERNSTEIN

Plaintiffs,

COMPLAINT

- against -

Index 156455-2025

COINBASE, INC.

Defendant.
----------X

Plaintiffs, Cynthia Garrett, Henry Gonzalez, Scott Chung, Curt Burns, David Cooper and Craig Bernstein by and through their undersigned attorneys, for their Complaint against Defendant hereby alleges as follows:

INTRODUCTORY STATEMENT

1. Coinbase and Bitcoin exemplify everything that is wrong with money, technology, and the law.

2. Bitcoin is marketed by Coinbase as a "currency" and "decentralized system", but in practice, it functions as neither. Bitcoin's value depends entirely on speculation, and its infrastructure is dominated by centralized platforms like Coinbase and other opaque actors who have unchecked, centralized, power.

3. Coinbase has positioned itself as a central authority in a lawless market, profiting from the fact that the government does not regulate Bitcoin like other investments, including stocks, bonds and mutual funds.

4. Unlike stocks, which rely on earnings to grow, Bitcoin's parabolic rise is driven by rumors, speculation, and half-truths. Since Bitcoin operates outside traditional regulatory frameworks, much of its narrative remains shrouded in mystery—fueling both fascination and volatility.

5. This lack of transparency poses a grave threat to financial stability, exposing millions of unsuspecting investors to potential fraud, systemic risk, and catastrophic losses.

6. Plaintiffs, many of whom are elderly, have suffered catastrophic financial losses and Coinbase is to blame.

7. Plaintiffs have collectively lost millions of dollars due to unauthorized withdrawals and theft from their accounts on Coinbase's platform. These losses are not isolated incidents, but part of a broader and ongoing cyber-war which has resulted in hundreds of millions of dollars in stolen crypto – all from Coinbase customers like Plaintiffs.

8. On May 15, 2025, Coinbase announced plans to reimburse investors for losses stemming from scams involving individuals impersonating Coinbase customer service representatives. As part of the announcement, Coinbase acknowledged that some of its own employees sold confidential customer information to hackers. While the company publicly pledged to reimburse all affected customers, that statement was a publicity stunt.[1]

9. In reality, Coinbase routinely denies reimbursement to victims of "customer service" scams and other qualifying losses covered under the Electronic Funds Transfer Act. Rather than supporting its customers, Coinbase often adopts an adversarial stance, effectively waging a second battle against the very users who trusted the platform to safeguard their Bitcoin.

[1] Available here: https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists

10. This is part of a broader legal strategy by Coinbase to curtail investor rights through its Terms of Service, which mandate a bifurcated dispute resolution process: some claims must be arbitrated, while others must be litigated in court. This contractual arrangement is part of a larger effort to insulate Bitcoin from public scrutiny and erode the due process rights of Bitcoin investors.

11. While Plaintiffs assert that Coinbase's customer agreement is procedurally and substantively unconscionable, they do not seek to invalidate it. Instead, Plaintiffs want to give Coinbase precisely what the parties "bargained for."

12. In this action, Plaintiffs hope to resolve a significant legal issue, whether Bitcoin is a "security" under *SEC v. Howey*, an important United States Supreme Court precedent, which established the test for what makes an instrument a security under federal law. Under *Howey*, an instrument is a "security" if it involves: (1) an investment of money, in; (2) a common enterprise, with; (3) an expectation of profits to be derived solely from the efforts of the promoter or a third party.

13. Individuals who purchase Bitcoin, including Plaintiffs, do so because they expect to make a profit from the efforts of others and for no other reason. Bitcoin qualifies as a security because its very existence and ongoing functionality relies on the efforts of third parties. These include not only "Bitcoin miners," who validate transactions and maintain the network, but also a centralized group of lead developers. This core team operates like a company with a well-defined corporate structure.

14. For this reason and others, it is the entire world's common understanding that Bitcoin is an investment and not a currency.

15. Bitcoin was only marketed as a "currency" because its founders were too scared

to label Bitcoin an "investment." According to a private email from Satoshi Nakamoto, Bitcoin's pseudonymous founder, "***"I'm uncomfortable with explicitly saying 'consider it an investment'…it's OK if they come to that conclusion on their own, but we can't pitch it as that***." Exhibit A, email 19. (emphasis added).

16. Bitcoin has never functioned as a currency and never will. Bitcoin is an investment and always will be.

JURISDICTION AND VENUE

17. Defendant regularly and systematically transact business in New York State, holding a "Bitlicense" through the New York State Department of Financial Services and having a main office address in New York County at 1350 Ave of the Americas, Fl 2 #1143, New York, NY 10019.

18. Jurisdiction and venue are proper in New York county because the parties contractually agreed that certain disputes would be heard in state Courts in New York, New York.

19. As of May 16, 2025, Coinbase's operative Terms of Service (the, "TOS") require that claims arising under the Securities Exchange Act must be brought in state or federal court located in New York, New York.

20. The terms of service, or "TOS", between the parties were last modified by Coinbase on April 10, 2025. The new TOS states, "[s]tarting May 15, 2025, the Arbitration Agreement will be updated to the version in Appendix 6. If you do not agree with this change, you can close your account and withdraw your funds by May 15, 2025."

21. Plaintiffs in this action all maintained accounts at Coinbase both before and after May 15, 2025. Plaintiffs also all filed individual arbitration cases (the, "Arbitration Cases")

against Coinbase before the American Arbitration Association. The Arbitration Cases seek particularized damages on behalf of each of the Plaintiffs. The TOS between Plaintiffs and Coinbase prohibit Plaintiffs from asserting certain claims in the Arbitration Cases.

22. Appendix 6 of the TOS, provides in relevant part:

> 5. Disputes about whether you or we have violated state or federal securities laws. In the event that there is a Dispute about whether you or we have violated state or federal securities laws, you and we agree that such Disputes shall be resolved by a court of competent jurisdiction. This means, for example, if you have a Dispute that contains causes of action under the state or federal securities laws and other causes of action that are arbitrable, then the arbitrable causes of action must proceed in arbitration and the state or federal securities laws causes of action must proceed in a court of competent jurisdiction.

23. The TOS further provides that state and federal courts in New York, New York will have "exclusive jurisdiction" over any dispute that is not filed in arbitration. The provision provides in relevant part:

> 9.10 Forum Selection. Unless you and Coinbase agree otherwise, to the maximum extent permitted by applicable law, the state and federal courts in New York, New York (except for small claims courts, in which case you and we agree to resolve our Disputes in a small claims court of competent jurisdiction) will have exclusive jurisdiction over any Dispute that is not subject to arbitration or over any action involving the applicability or enforceability of the Dispute Resolution section 7 or any portion of the Dispute Resolution section (including the Arbitration Agreement, Appendix 6). You and Coinbase consent to the exclusive jurisdiction of these courts and waive any objections as to: (1) personal jurisdiction or (2) the laying of venue in such courts because of inconvenient forum or any other basis or right to seek to transfer or change venue of any such action to another court.

PARTIES

24. Coinbase is a Delaware corporation founded in 2012. Coinbase has operated a crypto asset trading platform servicing U.S. customer since 2012. Coinbase's platform allows users to buy, sell, and trade crypto assets, including Bitcoin. Coinbase merges three functions

that are required to be legally segregated under the Securities and Exchange Act — those of brokers, exchanges, and clearing agencies.

25. Plaintiff, Cynthia Garrett, is a resident of California. Ms. Garrett is the owner of Cynthia Garrett Ministries and is a well-known media personality. Ms. Garret was the victim of a complex cyber theft, which resulted in Bitcoin and other cryptocurrency being stolen from her account at Coinbase. She has also purchased Bitcoin at Coinbase.

26. Plaintiff, Henry J. Gonzalez, is a resident of California. Dr. Gonzales is a 67 year old physician. He was the victim of a complex cyber theft, which resulted in over $3,400,000 in Bitcoin and other cryptocurrency being stolen from his account at Coinbase. He has also purchased Bitcoin at Coinbase.

27. Plaintiff, Scott Chung, is a resident of California. Mr. Chung was the victim of a complex cyber theft, which resulted in over $500,000 in Bitcoin and other cryptocurrency being stolen from his account at Coinbase. He has also purchased Bitcoin at Coinbase.

28. Plaintiff, Curt Burns, is a 69-year-old resident of Iowa. Mr. Burns was the victim of a complex cyber theft, which resulted in over $1,300,000 in Bitcoin and other cryptocurrency being stolen from his account at Coinbase. He also purchased Bitcoin at Coinbase.

29. Plaintiff, David Cooper, is an 85-year-old retiree from Florida. Mr. Cooper was the victim of a complex cyber crime, which resulted in over $110,000 in Bitcoin and other cryptocurrency being stolen from his account at Coinbase. He also purchased Bitcoin at Coinbase.

30. Plaintiff, Craig Bernstein, is a 71 year old resident of Florida. Mr. Bernstein was the victim of a complex cybercrime, which resulted in over $420,000 in Bitcoin and other cryptocurrency being stolen from his account at Coinbase. He also purchased Bitcoin at

Coinbase.

FACTS

I. HISTORY OF BITCOIN

A. Rumors and regulation

31. On October 31, 2008, a link to a white paper authored by "Satoshi Nakamoto" titled *Bitcoin: A Peer-to-Peer Electronic Cash System* was posted to a cryptography mailing list to generate interest in Bitcoin.

32. Satoshi Nakamoto means "wise central origin" in Japanese. [2]

33. While the Whitepaper purported to establish Bitcoin as a currency, privately "Satoshi Nakamoto" was looking for other ways to secretly monetize Bitcoin.

34. According to a private email from Nakamoto exchanged approximately nine months after Bitcoin's Whitepaper was released:

> It would help if there was something for people to use it for. ***We need an application to bootstrap it. Any ideas?*** There are donors I can tap if we come up with something that needs funding, but they want to be anonymous, which makes it hard to actually do anything with it.

(Exhibit A, Email 24) (emphasis added)

35. In response to this email, Bitcoin developer Malmi suggested that Bitcoin be could be monetized through an exchange, similar to Coinbase. Here is Malmi's reply with Satoshi's response:

> <Martiin Malmi> This exchange business thing is something that I'd be interested in doing, and I also have the sufficient technical skills to do it. Although, before this can be done, there should be a non-alpha version of Bitcoin (and the command line interface / API). ***If this gets started, donors / high-risk investors would be very***

[2] "Satoshi Nakamoto" was a pseudonym used by the creator of Bitcoin. The pronouns he/him will be used in this Complaint, but it is more likely that "Satoshi Nakamoto" was a group of individuals.

> ***welcome to bring capital for the currency's backup.*** So, what do you think about the idea? Note that this is not something that I'm asking you to do (unless you want to) if you're busy with other things. I can do it myself, if I get positive reviews about the plan.
>
> <Satoshi Nakamoto>: ***That's great, I could probably get a donor to send currency to you which you convert to euros and pay out through methods that are convenient for users***. I don't want to do an exchange business myself, but it can be done independently of me. Like you say, there is more software development to be done first, and also I'd like to keep trying for a while to think of a bootstrap application to use bitcoins for. I've had some ideas that could only be done before an exchange exists.

(Exhibit A, Email 28) (emphasis added)

36. As the above email and others indicate, Bitcoin was only ***marketed*** as a currency.

37. In reality, Bitcoin was created as an instrument used to speculate by participants in secondary markets like Coinbase.

38. The idea to create electronic cash using encryption was first introduced by the United States National Security Agency, or NSA, in 1996, through an academic paper. See Exhibit B.

39. At the time, the idea was called "NSA Mint." After the idea for NSA mint was published, other cryptographers came up with similar ideas.

40. The idea for NSA Mint was published even before the encryption technology securing Bitcoin was invented. That technology, SHA-256 encryption, was invented in 2002.

41. It was also invented by the federal government. See Exhibit C.

42. These unusual coincidences have led to public speculation that the NSA, or the central intelligence agency (CIA), created Bitcoin in 2008.

43. These, and other fantastic rumors, are synonymous with Bitcoin. Rumors also create the perfect environment for scammers to exploit innocent investors, including Plaintiffs.

44. Indeed, the issue raised by the Plaintiffs is so omnipresent in Bitcoin that even internet scammers are exploiting the law's ambiguity.

45. The next page of this Complaint is a screenshot from a common Coinbase scam, which attempts to trick victims into believing that a Court is requiring Coinbase to migrate wallets under the Securities and Exchange Act:

coinbase

As of March 14th, Coinbase is transitioning to self-custodial wallets. Following a class action lawsuit alleging unregistered securities and unlicensed operations, the court has mandated that users manage their own wallets. Coinbase will operate as a **registered broker**, allowing purchases, but all assets must move to **Coinbase Wallet**.

Your unique recovery phrase below is your Coinbase Identity. It grants access to your funds—write it down and store it securely. Import it into **Coinbase Wallet** by entering each word followed by a space.

1. **clarify**	2. **uncover**
3. **audit**	4. **behave**
5. **roof**	6. **industry**
7. **quote**	8. **marine**
9. **disease**	10. **invest**
11. **core**	12. **dragon**

Step 1: Set Up Your Wallet

- Download Coinbase Wallet as a mobile app or browser extension.
- Import your **recovery phrase** by selecting "I already have a wallet."

Step 2: Transfer Your Assets

- For each asset, click "Receive" in the wallet app/extension.
- Select "Receive from Coinbase."
- Choose "Add crypto with Coinbase Pay."
- Transfer all assets via Coinbase Pay.

No Time to Wait

Act quickly—the **deadline** to transfer your assets to a self-custodial wallet is **April 1st, 2025**.

Get Started Now

46. Unfortunately, these and other online scams are endemic to Bitcoin.

47. Even the federal government has created false online rumors about crypto. During the Biden administration, the SEC registered the domain www.HoweyCoins.com and "sold" Howey Coins in a bizarre effort to educate the public about crypto.

48. The "Howey Coin" website is down, but articles about it are still up on the SEC's website.[3] Here is a screenshot:

[3] Available here: https://www.investor.gov/ico-howeycoins

49. Bitcoin investors do not need more fake websites from the federal government. Bitcoin investors need recognition that Bitcoin is a security under federal law. Without this protection, the market will eventually lose confidence in Bitcoin and abandon the asset.

B. Bitcoin is three different things – a token, a network and software.

50. Individuals who invest in Bitcoin, purchase digital tokens, called "Bitcoins." "Bitcoin" is also the name of the network used transact the tokens. Finally, "Bitcoin" is the name of the software individuals must download to access the network.

51. The name "Bitcoin" is commonly used to refer to all three of these things – the token, the network and the software.[4]

52. Bitcoin transactions are recorded on a public ledger called the blockchain. The blockchain is functionally similar to an excel spreadsheet that cannot be modified because it is protected with encryption.

53. Bitcoin's encryption technology, SHA-256 encryption, is the key to keeping it secure.

54. SHA-256, like the wheels of a cipher, shifts messages through intricate steps, transforming an input into a complex fingerprint that is difficult, but not impossible to decrypt.

55. SHA-256 encryption is only made to sound complicated. In practice, SHA-256 follows simple steps. A message can be encrypted using SHA-256 on a single sheet of graph paper by hand.

56. Mathematically, SHA-256 should produce a random output that has 2^256 different outcomes. Because SHA-256 produces such a large output, it cannot be cracked using a method like brute force guessing because that would require too much computer power and

[4] In 2014, the name of Bitcoin's software was changed from Bitcoin to Bitcoin Core.

take too long.

57. However, other methods to defeat SHA-256 have proven effective. Exhibit D.

C. How is Bitcoin "mined?"

58. Traditionally, when an individual transfers a Bitcoin token to someone, the transaction needs to be verified before it is added to Bitcoin's public spreadsheet. This process is known as mining.

59. Bitcoin would not exist, but for the efforts of third parties, called "miners."

60. Miners solve complex cryptographic puzzles using "protocols" that are designed to prevent manipulation of Bitcoin's public spreadsheet. "Protocols" are standardized rules that are written into the computer code running Bitcoin's software.

61. Miners make money, not by solving the puzzle, but by being rewarded with Bitcoin for coming closest to the answer. Bitcoin mining is like thousands of players racing to roll a 10,000-sided die—the first to land closest to a pre-defined answer wins and the game resets. Like a dice game, each one of the players should have an equal chance of winning.

62. However, miners with more computer power can hack Bitcoin because they can generate substantially more rolls of the dice. This means that miners with more computer power have a higher chance of "winning."

63. It is analogous to a player rolling their dice many billions of times more than any other player.

64. Because of this feature, a single node with sufficient computing power could overtake Bitcoin and hack its spreadsheet. For this reason, Bitcoin would not exist, but for the continued computational efforts of honest third-party miners. If honest miners stopped working, so would Bitcoin. Their efforts are essential to Bitcoin's existence and profitability.

65. Bitcoin also requires other, necessary third parties, including Bitcoin's lead developers, all of whom work to maximize Bitcoin's profitability.

66. The efforts of these centralized third parties are ongoing. If their efforts stop, so will Bitcoin both as a network and a token.

67. The same is true for Bitcoin, as a software. The code is not static, and Bitcoin's continued success is entirely dependent on its code being updated and modernized.

68. Bitcoin is constantly under attack by hackers, and it requires a paid staff of developers to keep it safe and correct vulnerabilities quickly and efficiently.

69. In addition to correcting vulnerabilities, modifications to Bitcoin's code are periodically made to make Bitcoin's software more marketable and user friendly.

70. Because of these constant changes, Bitcoin's code is materially different today than in 2008 when it was released. Since it was first released, there have been hundreds of thousands of additional lines of code added to Bitcoin.

71. By its express policy, those lines of code can only be added by a small number of developers who are led by a lead developer.

72. As discussed below, but for the ongoing efforts of these developers, Bitcoin would not exist.

D. Who controls Bitcoin's Software?

73. Traditionally, only five or fewer developers have the password to Bitcoin. Other individuals can suggest changes, but only Bitcoin's small development team can actually change Bitcoin's code.

74. There have only been three lead developers in Bitcoin's history – Satoshi Nakamoto (2008 – 2010), Gavin Andresen (2010-2014) and Wladimir van der Laan (2014-

present).

75. Bitcoin's development team can, and often does, modify Bitcoin's code without the consent or even knowledge of Bitcoin's users and/or miners. Because Bitcoin's development team can act in this fashion, it means Bitcoin does not really use "consensus" or "voting."

76. It also means Bitcoin is "centralized" rather than "decentralized."

77. An example of such a centralized code modification occurred in 2018, after Bitcoin's lead developers were anonymously warned that Bitcoin's code could be manipulated to allow more than 21 million Bitcoin to be "mined". At the time, the lead developer made the decision to keep the vulnerability a secret and to notify Bitcoin miners after it was fixed.

78. This was the second time in Bitcoin's history that a hacker was able to exploit Bitcoin's inflation bug. The other time was in 2010 when a hacker successfully created 184 billion Bitcoin. [5]

79. Here is the public notice, which was posted after the code was changed in 2018:

> In order to encourage rapid upgrades, the decision was made to immediately patch and disclose the less serious Denial of Service vulnerability, concurrently with reaching out to miners, businesses, and other affected systems while delaying publication of the full issue to give times [sic] for systems to upgrade. On September 20th a post in a public forum reported the full impact and although it was quickly retracted the claim was further circulated.[6]

80. In the above example, users were notified of a critical modification to Bitcoin's

[5] See disclosure of CVE-2010-5139
Available here: https://www.cve.org/CVERecord?id=CVE-2010-5139

[6] See Disclosure of CVE-2018-17144
Available here: https://bitcoincore.org/en/2018/09/20/notice/

code only after downloading, installing and running the new version.

81. Bitcoin users are forced to constantly upgrade Bitcoin's software with hidden updates because prior version of Bitcoin's software have "end of life," or "EOL" dates, necessitating users to download new versions of Bitcoin's software.

82. Bitcoin's public policies and procedures state that its code could be changed in this manner (i.e. without notice and with forced EOL dates). If a vulnerability is identified, Bitcoin's code is changed and Bitcoin users are notified up to one year later.

83. Here is the policy:[7]

***

When reported, a vulnerability will be assigned a severity category. We differentiate between 4 classes of vulnerabilities:

- Low: bugs which are hard to exploit or have a low impact. For instance a wallet bug which requires access to the victim's machine.

- Medium: bugs with limited impact. For instance a local network remote crash.
- High: bugs with significant impact. For instance a remote crash, or a local network RCE.
- Critical: bugs which threaten the whole network's integrity. For instance an inflation or coin theft bug.

Low severity bugs will be disclosed 2 weeks after a fixed version exists on the current major release branch. A pre-announcement will be made at the same time as the release.

Medium and High severity bugs will be disclosed 2 weeks after the last affected release goes EOL [end of life]. This is a year after a fixed version was first released. A pre-announcement will be made 2 weeks prior to disclosure.

Critical bugs are not considered in the standard policy, as they would most likely require an ad-hoc procedure. Also, a bug may not be considered a vulnerability at all. Any reported issue may also be considered serious, yet not require embargo.

***

84. Bitcoin is "consensus" in name only because, as the above policy indicates, its code can be changed in secret, by a centralized authority, with users only being notified after a

[7] Available here: https://bitcoincore.org/en/security-advisories/

change occurs.

E. Bitcoin under "Satoshi Nakamoto."

85. The early marketing of Bitcoin was organized and deliberate.

86. Bitcoin's first lead developer was an internet persona who used the pseudonym Satoshi Nakamoto.

87. This pseudonym means "wise central origin" in Japanese.

88. Although significant effort has been made to dox him, Nakamoto's identity is still not known to the public. If he is a person, his individual net worth could be more than $100 billion, making him one of the richest people in the world.

89. Beginning in 2008, Nakamoto began trolling various internet message boards to post about digital currency. Through these efforts, Nakamoto recruited investors, computer programmers and a marketing team for Bitcoin.

90. One of the first individuals Nakamoto recruited to assist in the marketing of Bitcoin was a 19-year-old college student from Finland named Martti Malmi.

91. The pair met on an anti-state website in 2009.

92. Only two weeks after meeting Malmi, Satoshi Nakamoto gave him access to Bitcoin's public website. Nakamoto instructed Malmi, a Finish-national, to create an English language "frequently asked questions" for Bitcoin.

93. Nakamoto, whose written English was superior to Malmi's, offered the following legal advice to Malmi about translating the website into Finish, Malmi's native language, "[o]ften the standard answer about legalities is that it's only intended for people in other countries. Translating it into your home language weakens that argument." See Exhibit A, Email 158.

94. Nakamoto, intent on evading laws, offered other legal advice to Malmi.

95. When Malmi referred to Bitcoin as an "investment" on its first website, Nakamoto corrected him, "I'm uncomfortable with explicitly saying 'consider it an investment'. That's a dangerous thing to say and you should delete that bullet point. It's OK if they come to that conclusion on their own, but we can't pitch it as that." Exhibit A, Email 19.

96. Malmi, under the direction of Nakamoto, always complied with orders. As lead developer, Nakamoto was effectively the de-facto CEO of Bitcoin.

97. As its CEO, Nakamoto recruited Malmi and others to help him run Bitcoin like an organized business with a defined structure.

98. Malmi was also asked by Nakamoto to serve as Bitcoin's first treasurer. According to a 2010 email from Nakamoto to Malmi: "BTW, it's looking like I may be able to get us some money soon to cover web host costs, back your exchange service, etc, ***in the form of cash in the mail***. Can you receive it and act as the project's treasurer?" Exhibit A, Email 193 (emphasis added).

99. As treasurer, Malmi paid web hosting costs for Bitcoin's first website and facilitated money exchange services for Nakamoto and other individuals, who mailed physical currency (USD) to Malmi in Finland.

100. According to a June 25, 2010 email from Nakamoto to Malmi, "I got a donation offer for $2000 USD. I need to get your postal mailing address to have him send to. And yes, he wants to remain anonymous, so please keep the envelope's origin private." Exhibit A, Email 195.

101. The key to Bitcoin's early success was absolute secrecy about Bitcoin's real founders – investors who mailed currency to Finland and other locations around the world.

102. Additional private emails between Nakamoto and Malmi confirmed that physical currency was mailed to Malmi to support the early adoption of Bitcoin. This physical currency was sent by Satoshi Nakamoto as well as other third-parties, whose anonymous investments of green cash propped up the early value of Bitcoin.

103. But for Malmi and other third parties, including those who sent him physical currency, there would be no Bitcoin.

104. Between 2009 and 2011, Malmi worked with Nakamoto to market Bitcoin and increase its profitability.

105. Malmi publicly maintains that he ceased all involvement with Bitcoin in 2011.

106. In 2024, he released his private emails with Satoshi Nakamoto through a post on www.x.com. Those emails were previously unknown to the public and Plaintiffs.

F. Nakamoto gives Bitcoin's password to Gavin Andresen (2010).

107. By the end of 2010, Nakamoto began planning his exit from Bitcoin and public life.

108. On December 3, 2010, Malmi asked Nakamoto who should receive the password to Bitcoin. This is the private email exchange between Nakamoto and Malmi:

> Malmi: I could give the root password to you and somebody else. Xunie has volunteered, but we might find somebody even more professional from the forum and keep the number of admins at the minimum. If the outage was due to heavy load, he could help us move to lighttpd or optimize resources otherwise. Should we make a recruitment thread on the forum?
>
> Nakamoto: It should be Gavin. I trust him, he's responsible, professional, and technically much more linux capable than me. (I don't know Xunie, but he hasn't posted for months and he was a goofball)

Exhibit A, Email 241.

109. After this email exchange in December 2010, Gavin Andresen became the lead developer of Bitcoin.

110. Having the root password to Bitcoin, gave Andresen the ability to unilaterally change the code for Bitcoin. Andresen, like Nakamoto and Malmi, had complete and total control over Bitcoin.

111. In 2011, before allegedly disappearing, Nakamoto also asked Andresen to serve as Bitcoin's spokesperson. Since that time, Andresen has been far more than just a vocal public advocate for Bitcoin.

112. During his tenure as lead developer, Andresen added 62,000 lines of code to Bitcoin and removed 76,000 – materially changing Bitcoin from the software that Nakamoto allegedly first coded.

113. In 2012, and in an effort to provide legitimacy to Bitcoin, Andresen also created an organization called the "Bitcoin Foundation."

114. Like Bitcoin itself, the Bitcoin Foundation was funded through significant anonymous donations of money. It was initially created as a not-for-profit, but its tax-exempt status was revoked by the IRS in 2022.

115. Andresen used the Bitcoin Foundation to create a more centralized and organized authority for Bitcoin. This is a stark contrast from the public image of "decentralization," which Bitcoin attempts to portray.

116. Through the foundation, Andresen began paying himself a salary in Bitcoin. He also hired a staff of other coders, all of whom were paid with Bitcoin. Because these individuals were paid with Bitcoin, they had a financial stake in the success of Bitcoin.

117. As the years went on, Bitcoin became more centralized through the foundation.

By 2012, Bitcoin was operating more like a well-run company and less like a decentralized technology.

118. Bitcoin not only had a defined corporate structure with equity employees -- it also had lawyers and even its own DC lobbyists.[8]

119. All these individuals were using their specialized skills to maximize the profitability of Bitcoin.

120. But for the specialized efforts of Bitcoin's employees, lawyers and lobbyists, Bitcoin would not have increased in value.

G. Andresen steps down (2014)

121. Things were going reasonably well for Bitcoin until 2014, when several high-profile scandals rocked it. These scandals include the arrest of one of the board members of the Bitcoin Foundation for money laundering.

122. Bitcoin was also hacked, a second time, in 2014. During this hack, Satoshi Nakamoto's email address, satoshin@gmx.com, was hacked and the hacker was able to use it to communicate with reporters. The hacker viewed Satoshi Nakamoto's old emails and even proved they were able to read them by forwarding them. It was an extremely serious security breach.

123. Using Nakamoto's credentials, the hacker also compromised the website containing Bitcoin's source code. The hacker temporarily changed Bitcoin's name to "Buttcoin," but took no other malicious action. The hacker could have, but did not, insert

[8] Bitcoin Foundation to Ramp Up Lobbying Efforts, *Wall Street Journal*, March 11, 2014

Available here: https://www.wsj.com/articles/bitcoin-foundation-hires-cato-institute-official-jim-harper-1394500176

malicious code into Bitcoin.

124. The same year, 2014, Gavin Andresen stepped down as Bitcoin's lead developer and appointed an individual named Wladimir van der Laan, a Dutch computer scientist.

125. In 2016, Wladimir van der Laan had a public falling out with Gavin Andresen and revoked Andresen's ability to make changes to Bitcoin. The falling out concerned false public statements Andresen made about the identity of Satoshi Nakamoto. Essentially, Andresen was tricked into publicly declaring that a con-artist was Satoshi Nakamoto.

126. van der Laan apparently no longer trusted Andresen with Bitcoin's password because he feared Andresen would share it with an imposter posing as Nakamoto. Due to this fear, Andresen's Bitcoin privileges were publicly revoked and his password was disabled.9

127. Andresen was effectively banned from contributing to Bitcoin by his appointed successor, a fact which further highlights that Bitcoin will always be controlled by one person – its lead developer and de-facto CEO.

128. Since 2016, Bitcoin continues to operate in an even more autocratic fashion. After van der Lann was appointed lead developer, webpages were scrubbed from Bitcoin's website and its internal operation became even more secretive.

129. Bitcoin continues to be controlled by five or fewer "maintainers" who can, and often do, modify Bitcoin's code without any advance notice.

[9] "Dazed and confused", by Wladimir van der Lann a/k/a "Laanwj," dated May 6, 2016 Available here: https://laanwj.github.io/2016/05/06/hostility-scams-and-moving-forward.html

H. Where does Bitcoin come from?

130. When Bitcoin was first created, there were no Bitcoins in existence. The only way to bring new Bitcoins into circulation is through the "mining process", described above.

131. Bitcoin's mining process was allegedly designed to reduce the amount of Bitcoin awarded to miners based on a fixed schedule, called "halving," which reduces mining rewards by 50% every four years.

132. The alleged purpose of "halving" is to limit the supply of Bitcoin to 21 million, at which point Bitcoin mining will be supported by transaction fees.

133. As a result of Bitcoin's "halving protocol," approximately 50% of Bitcoin's total supply was mined before 2012.

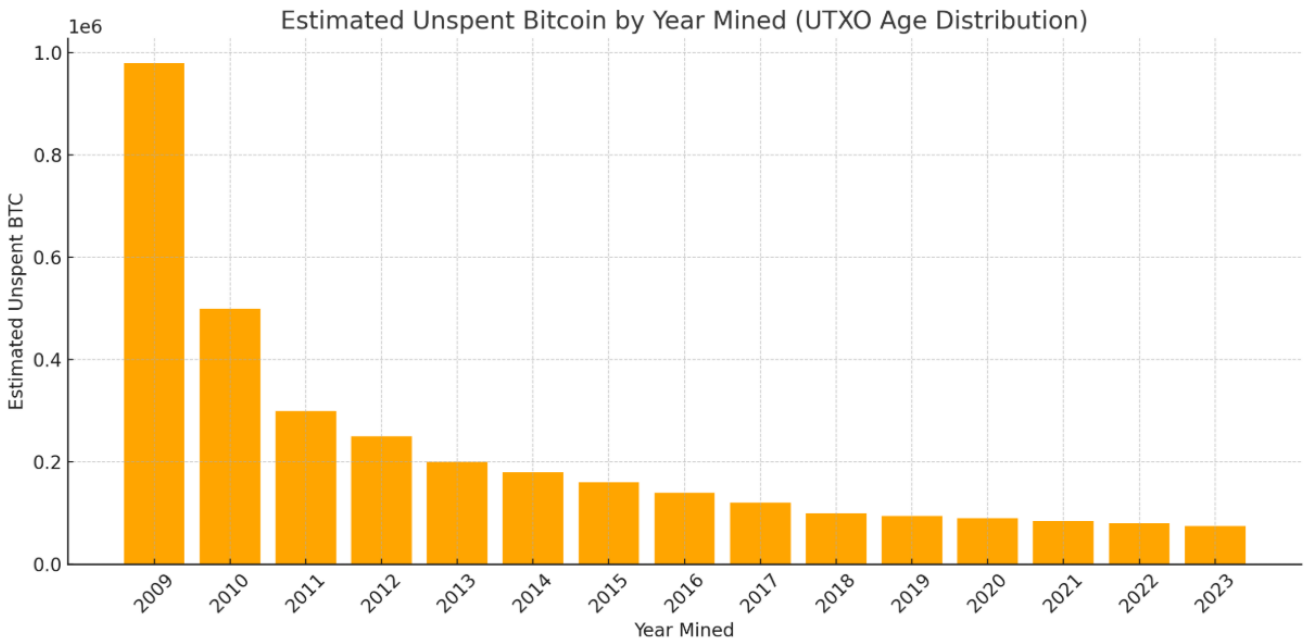
134. Here is the schedule of Bitcoin's release based on its halving protocol:

Period	Year	Block Reward (BTC)	New BTC Created	Cumulative Supply	% Supply
Genesis	2009	50 BTC	10,500,000	10,500,000	50.00%
1st Halving	2012	25 BTC	5,250,000	15,750,000	75.00%
2nd Halving	2016	12.5 BTC	2,625,000	18,375,000	87.50%
3rd Halving	2020	6.25 BTC	1,312,500	19,687,500	93.75%
4th Halving	2024	3.125 BTC	656,250	20,343,750	96.88%
5th Halving	2028	1.5625 BTC	328,125	20,671,875	98.44%
6th Halving	2032	0.78125 BTC	164,063	20,835,938	99.22%
7th Halving	2036	0.390625 BTC	82,031	20,917,969	99.61%
8th Halving	2040	0.1953125 BTC	41,016	20,958,984	99.80%
...	...	...	...	...	
Final Bitcoin	~2140	0 BTC	~0	21,000,000	

135. There has been public speculation that Satoshi Nakamoto owns or controls upwards of more than 1 million Bitcoin, which was mined before 2012. Again, like other aspects of Bitcoin, speculation about how much Bitcoin is owned by Satoshi Nakamoto cannot be verified with any reliable methods.

136. The only thing that can be ascertained with mathematical certainty is the total amount of unspent Bitcoin from that period – not who owns or mined it.

137. Bitcoin can be studied to ascertain if it was ever spent by looking at a value known as the unspent transaction output, or UTXO. An analysis of this data shows that approximately 15% of Bitcoin's total supply, or 3 million Bitcoin were mined before 2012 and remain unspent. Here is a chart showing unspent Bitcoin by year mined:



138. If Bitcoin were a stock, individuals holding more than 5% would be required to disclose their identity and trading records to the SEC. This ensures that insiders do not engage in market manipulation, as their large ownership stake allows them to influence the market and cheat.

139. For Bitcoin, the identity of the owners of at least 15% or more of its outstanding supply remains anonymous.

140. This is an incredible risk to the integrity of Bitcoin.

II. COINBASE MARKETS BITCOIN AS AN INVESTMENT

A. Coinbase Markets Bitcoin as an "Investment."

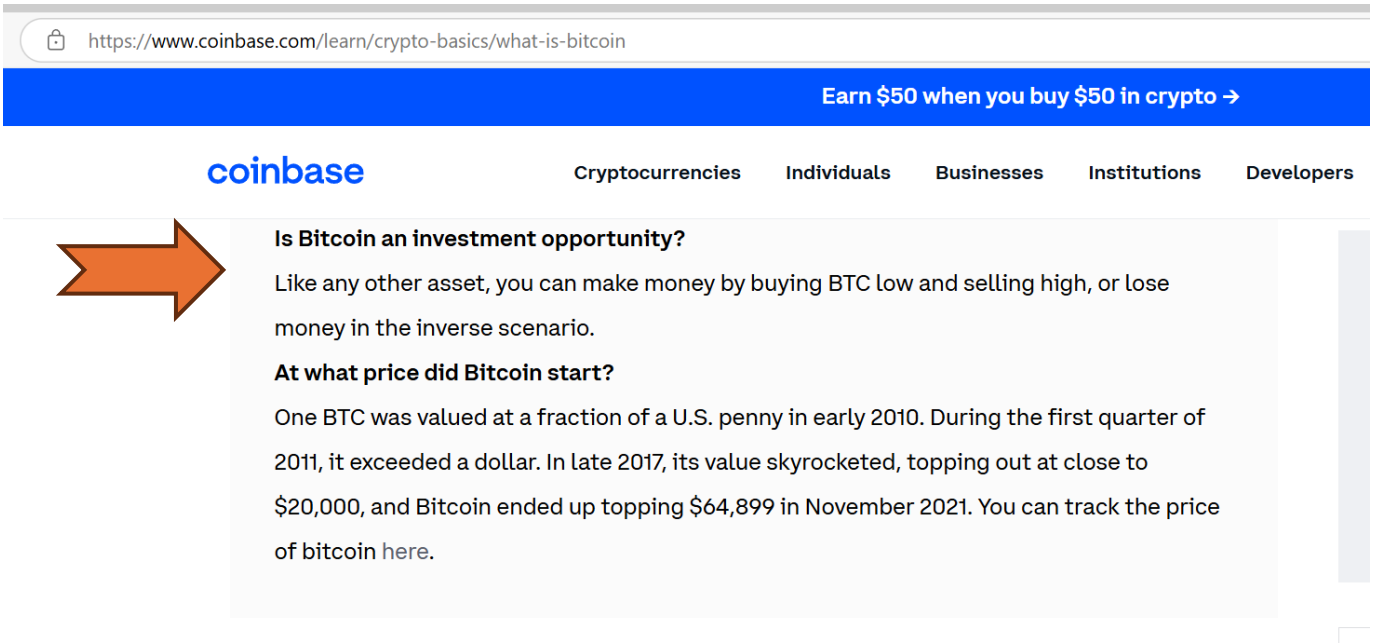
141. Coinbase has filled the role of America's largest Bitcoin exchange – facilitating an untold number of transactions in the world's largest unregulated stock market.

142. Defendant operates Coinbase as a centralized exchange to buy and sell cryptocurrencies, including Bitcoin. Coinbase operates like a brokerage firm and stock exchange combined. It is a very dangerous conflict of interest.

143. Coinbase markets Bitcoin as an investment, not a currency, through statements made on its public website www.Coinbase.com and those made by Coinbase's CEO on www.X.com. Those statements and all the pages of www.coinbase.com are incorporated by reference herein.

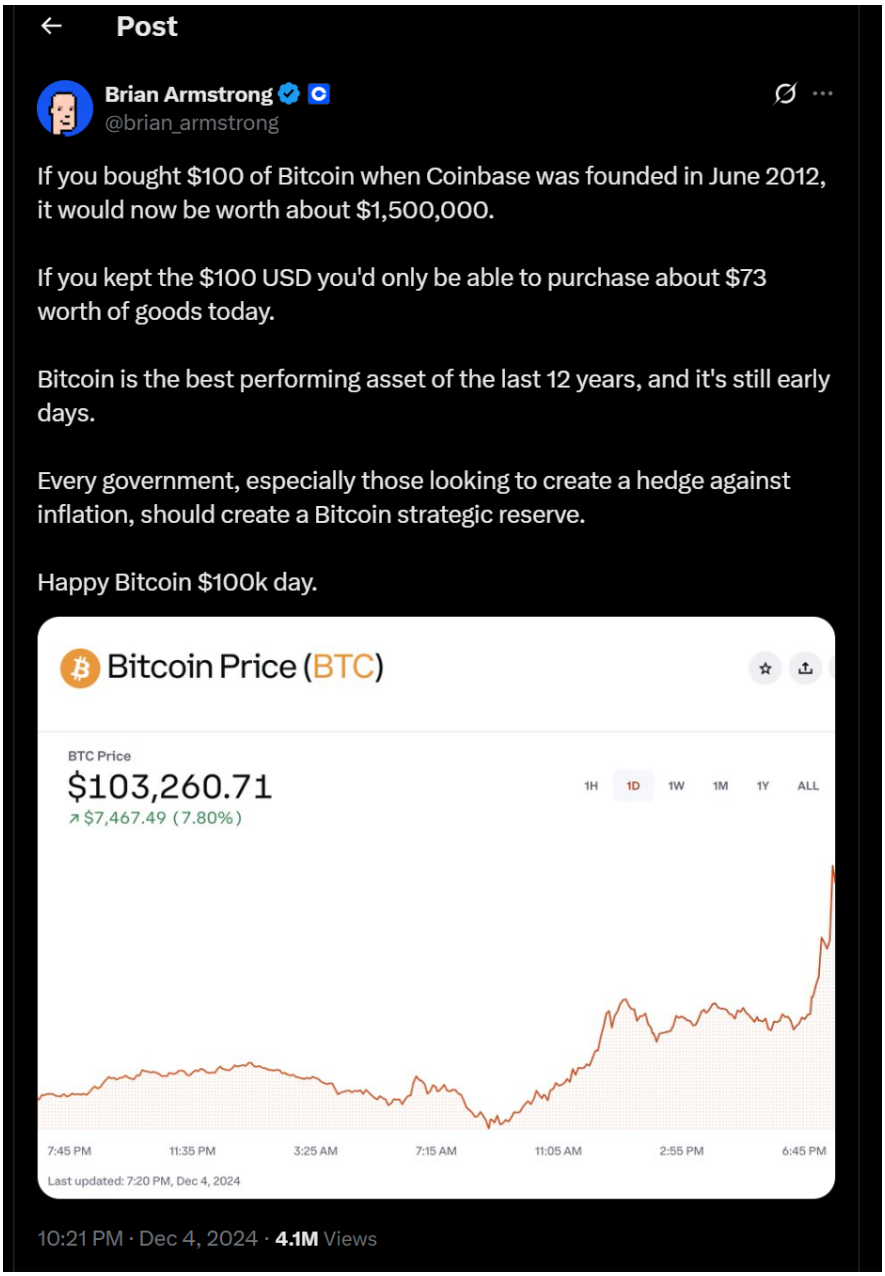
144. Coinbase, unlike Satoshi Nakamoto, is not reserved about marketing Bitcoin as an investment or using the word "investment" to describe Bitcoin.

145. Here is one example of how Coinbase markets Bitcoin:



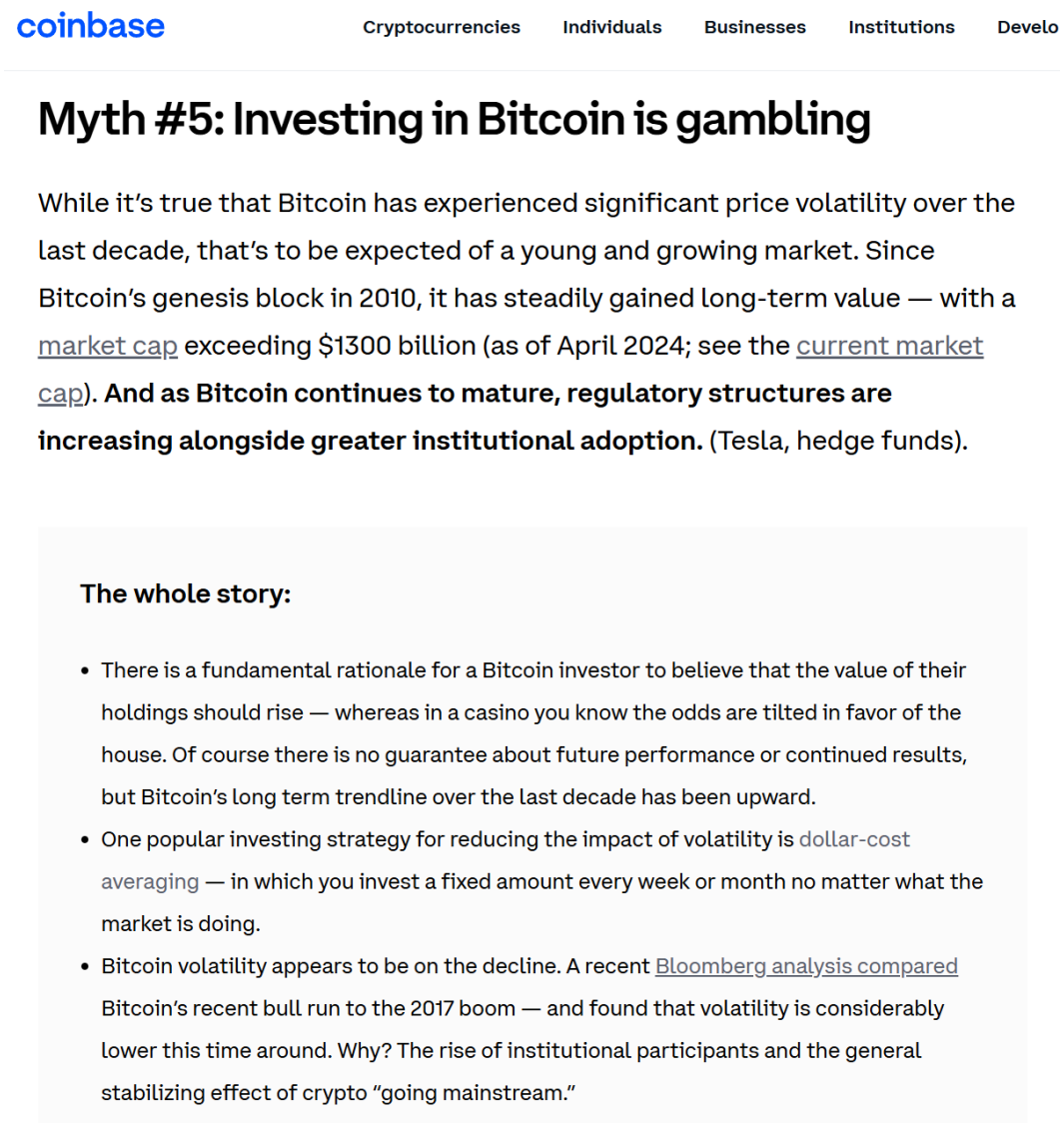
146. The foregoing investment projection is confusing. It is also devoid of any disclaimer or other qualifying language. This chart is inherently and materially misleading.

147. Coinbase's CEO routinely posts similar misleading posts on www.X.com about Bitcoin, including a post which claimed that a $100 investment in Bitcoin made in June 2012, could have appreciated to $1,500,000 by December 4, 2024:



148. Similar to the posts on www.Coinbase.com, Coinbase's CEO's posts on X.com are materially misleading. Specifically, the post does not provide any real details about the projection, including the actual purchase price or date.

149. Coinbase's website also explicitly states that individuals invest in Bitcoin because there is a "fundamental rationale for a Bitcoin investor to believe that the value of their holdings should rise."[10]



[10] Available here: https://www.coinbase.com/learn/crypto-basics/7-biggest-bitcoin-myths

150. Incredibly, even the fine print on Coinbase's website refers to cryptocurrency as "investments."

151. Here is an example from Coinbase's TOS, "you are solely responsible for determining whether any ***investment, investment strategy or related transaction is appropriate for you based on your personal investment objectives***, financial circumstances and risk tolerance." (emphasis added).

152. While Coinbase's website discusses Bitcoin as an investment opportunity, it does not discuss any of the ongoing issues concerning technical flaws in Bitcoin. It also does not discuss any of the technical innovations or positive coding changes to Bitcoin.

153. Instead, Coinbase clearly markets Bitcoin as an investment and not as a technology or even as a currency. The entire focus of the substance of the marketing is on investing.

B. Coinbase Makes False Statements and Omissions about Bitcoin.

154. Coinbase makes a number of materially false statements concerning Bitcoin and cryptocurrencies on its public website, which was reviewed and relied on by the Plaintiffs.

155. Specifically, Coinbase makes the following false statements about Bitcoin:

Statement	Why false?
"There will only ever be 21 million Bitcoin. This is digital money that cannot be inflated or manipulated in any way."[11]	First, Bitcoin's inflation cap was hacked in 2010 and 184.4 billion Bitcoins were successfully minted. In 2018, a second vulnerability was identified and corrected. Second, there are "tokenized" and "securitized" versions of Bitcoin, which trade on a 1:1 basis with Bitcoin. These products inflate the supply of Bitcoin well above 21 million.

[11] Available here: https://www.coinbase.com/learn/crypto-basics/plp-what-is-bitcoin

"Every transaction involving Bitcoin is tracked on the blockchain, which is similar to a bank's ledger, or log of customers' funds going in and out of the bank. In simple terms, it's a record of every transaction ever made using bitcoin."[12]	Most Bitcoin transactions on Coinbase are conducted "off chain" in a secret ledger that is controlled and maintained by Coinbase. It is functionally similar to a dark pool. Coinbase maintains an entirely separate, and secret, ledger for these Bitcoin transactions.
"…all Bitcoin transactions happen on an open blockchain, it's often easier for authorities to track illicit activity than it would be in the traditional financial system."[13]	Bitcoin is **not** easier to trace than funds that are stolen in the traditional banking system. Plaintiffs, all victims of Bitcoin theft, know too well that Bitcoin transactions are not traceable for a variety of reasons.
"Bitcoin cannot be hacked."[14]	Bitcoin has been hacked multiple times. First, in 2010, hackers were able to successfully mint more than 184.4 billion Bitcoin. Second, in 2014, Bitcoin's website and Satoshi Nakamoto's emails were hacked. This hacker may also have access to passwords to some or all of Nakamoto's original wallets. Third, Bitcoin can be hacked by a single PC if it has more computer power than the rest of the computers on Bitcoin's network.

156. In addition to these misrepresentations, Coinbase omits three key material risks regarding Bitcoin on its website. Those risks are detailed below:

S-1 Risk 1: If Satoshi Nakamoto is identified or his Bitcoins are transferred, the value of Bitcoin will decline significantly.

[12] Id.
[13] Available here: https://www.coinbase.com/learn/crypto-basics/7-biggest-bitcoin-myths
[14] Id.

S-1 Risk 2: Developments in mathematics, technology, including in digital computing, algebraic geometry, and quantum computing could result in the cryptography being used by Bitcoin becoming insecure or ineffective.

S-1 Risk 3: Governance issues by Bitcoin's core developers could lead to revisions to the code or inactions that negatively affect Bitcoin's speed, security, usability, or value.

157. The foregoing risks about Bitcoin were paraphrased from Coinbase's S-1, the document Coinbase filed to become a public company.

158. Coinbase disclosed these risks about Bitcoin to investors in its IPO, because they were deemed by Coinbase to be material risks about Bitcoin. Coinbase even served its S-1 disclosures on Satoshi Nakamoto through the wallet address associated with Bitcoin's first block, "1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa". See Exhibit E.

159. ***It is hard to fathom how the federal securities laws could have required Coinbase to make disclosures about Bitcoin to Satoshi Nakamoto, but not its own customers.***

160. There are additional risks about Bitcoin that are omitted from both Coinbase's website as well as its public S-1. Those risks are as follows:

Additional Risk 1: Bitcoin is pseudo-anonymous because user's private information can be learned by studying the blockchain. The blockchain is like a bank that posts everyone's account balance online together with complex clues to find the account holder's identity. When users transact Bitcoin, each new transaction leaves more small clues which can be studied to expose "crypto whales." Once identified, crypto whales become high profile targets for hackers. [15] This

[15] Mark Cuban lost nearly $900,000 to crypto hackers—how investors can avoid similar scams, CNBC, September 21, 2023

Available here: https://www.cnbc.com/2023/09/21/mark-cuban-lost-nearly-900000-dollars-to-crypto-hackers.html

flaw was recognized by Nakamoto early on:

> It's possible to be pseudonymous, but you have to be careful. If someone digs through the transaction history and starts exposing information people thought was anonymous, the backlash will be much worse if we haven't prepared expectations by warning in advance that you have to take precautions.

Exhibit A, Email 197.

Additional Risk 2: Bitcoin is quasi-anonymous because some foreign users' identity can be completely shielded from a lawfully issued subpoena. In the United States, all owners of Bitcoin must comply with the Bank Secrecy Act and the United States Patriot Act. This means, with no lawful exception, every American who owns Bitcoin must provide their personal identifying information to their cryptocurrency exchange. This information is known as "know your customer" information, or KYC. Coinbase, and other centralized exchanges, collect KYC for their users and must provide this information in response to a lawfully issued subpoena. Foreign users of Bitcoin do not have to provide KYC information to a central authority, and their identity can never be ascertained by a subpoena. This feature of Bitcoin makes it unfair to Americans, who are increasingly being victimized by anonymous scammers living outside of America's jurisdiction.

Addition Risk 2: Bitcoin operates in a manipulated market. Due to the current state of the law, tactics that are illegal in the stock market are frequently employed in the Bitcoin markets. One example is "spoofing." Spoofing involves placing and then immediately canceling large orders to trick other traders. The practice has been illegal in the stock market for years, but remains a common "legal" way Bitcoin is manipulated. [16]

[16] A Vanishing $212M Bitcoin Order Caused Chaos for Traders. Is Spoofing Back in Crypto?, Coindesk, April 29, 2025

Additional Risk 3**:** At least 15% or more of the outstanding supply of Bitcoin is owned by anonymous wallets. These wallets can influence the price of Bitcoin.

Additional Risk 4: The US Government, through the NSA, has a clandestine way to compromise Bitcoin. This risk is reputational as well as actual. On June 16, 2010, an internal memorandum from the United States government detailed a clandestine government project known as "Project Bullrun." The memorandum disclosed that the government, through the NSA, had the ability to defeat encryption technology. According to the memorandum, which is attached hereto as Exhibit F:

> Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network technologies. BULLRUN involves multiple sources, all of which are extremely sensitive…[b]ecause of the multiple sources involved in BULLRUN activities, "capabilities against a technology" does not necessarily equate to decryption.

161. The Plaintiffs would not have invested in Bitcoin had they known the ugly truth about it.

Available here: https://www.coindesk.com/business/2025/04/29/a-vanishing-usd212m-bitcoin-order-caused-chaos-for-traders-is-spoofing-back-in-crypto

PLAINTIFF'S CAUSES OF ACTION
COUNT I
(DECLARATORY JUDGEMENT)

162. Plaintiffs incorporate by reference and repeat and reallege every preceding paragraph of the Complaint as if fully set forth herein.

163. An actual case or justiciable controversy exists between the Plaintiffs and Defendant concerning the status of Bitcoin as a "security" under the Securities and Exchange Act of 1933 and 1934 and the test established by *SEC v. Howey Co*., 328 U.S. 293 (1946).

164. As the United States Supreme Court noted in *Howey*, Congress defined "security" broadly to embody a "flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits." 328 U.S. at 299.

165. Since *Howey*, Courts have found novel or unique investment vehicles to be investment contracts, including those involving orange groves, animal breeding programs, cattle embryos, mobile phones, enterprises that exist only on the internet, and even other crypto assets.

166. Despite many public hearings over multiple administrations, Congress has not passed any laws to address whether Bitcoin should be included in the definition of a "security" in the Securities and Exchange Act of 1933 and 1934.

167. Instead of Congress acting, the Securities and Exchange Commission has offered years of confusing public "guidance" about whether Bitcoin and other cryptocurrencies constitute investments under federal law.

168. The SEC's guidance is not law and has done more investor harm than good. It is academic, ambiguous and downright confusing.

169. The SEC took decisive action on June 2023, when it finally sued Coinbase and

other major cryptocurrency exchanges. In its complaint, the SEC alleged that Coinbase's business of intermediating transactions in cryptocurrency constituted the operation of an unregistered brokerage firm in violation of federal securities laws. If successful, the SEC would have effectively shut down Coinbase.

170. On March 27, 2024, Coinbase lost a significant motion in the case. On that date, the United States District Court ruled against Coinbase and held that most cryptocurrencies were "securities" under the Securities and Exchange Act. The District Court determined this to be an important threshold issue and did not rule on whether Coinbase was an unlicensed brokerage firm. That issue was not reached.

171. On January 7, 2025, the District Court granted a request by Coinbase for the Second Circuit to review the District Court's March 27, 2024 decision on an interlocutory basis.

172. On February 27, 2025, the Securities and Exchange Commission, now under the direction of President Trump, abruptly dismissed the litigation against Coinbase.

173. After the dismissal, Coinbase issued a statement, which argued the case was motivated by "political leadership." Coinbase called the dismissal a "win for the rule of law."[17]

174. After dismissing these litigations, the SEC announced the creation of a "taskforce" to create rules for cryptocurrency, but no formal agency rules have been announced.

175. President Trump's cryptocurrency taskforce is organized and operating in exactly the same manner as President Biden's cryptocurrency task force. While the person sitting in the oval office has changed, nothing else has.

176. Both political parties continue to fail Bitcoin investors and their failure is only

[17] "Righting a major wrong", available here: https://www.coinbase.com/blog/righting-a-major-wrong

exacerbated by the inconsistent, and politically motivated, reactions of state-level securities regulators.

177. After the SEC dismissed its litigation, states with securities regulators who are politically aligned against President Trump, announced new lawsuits in response to the "regulatory void."[18] At the same time, other states who are allied with President Trump dropped their lawsuits, citing the task force.

178. The status of the law has gone from confusing, under Biden, to transactional, under Trump.

179. What has not changed are the losers – Bitcoin investors, like Plaintiffs.

180. It is entirely possible that a new political administration could change course a third time and re-charge Coinbase. It is also possible that crypto could become an "investment" in one state, but not others.

181. The law should not be this confusing, chaotic or transactional.

182. Bitcoin investors, more than any others, need the full protection of the Federal and State securities laws. Without basic investor protection, Bitcoin will cease to exist because rational market actors will eventually abandon Bitcoin.

183. Plaintiffs all have a preexisting legal dispute with Coinbase concerning Bitcoin or other cryptocurrency that were stolen from their accounts. The issuance of declaratory relief by this Court will terminate some or all of the existing controversy between the parties, and will provide certainty to the parties with respect to their rights and obligations under the Securities

[18] "States must fill enforcement vacuum being left by federal regulators who are abandoning these cases under Trump administration" Oregon Department of Justice, April 18, 2025

Available here: https://www.doj.state.or.us/media-home/news-media-releases/oregon-attorney-general-rayfield-sues-coinbase-for-promoting-and-selling-high-risk-investments/

and Exchange Act of 1933 and 1934.

COUNT II
VIOLATION OF FEDERAL SECURITIES ACT

184. Plaintiffs incorporate by reference and repeat and reallege every preceding paragraph of the Complaint as if fully set forth herein.

185. According to The Securities Act of 1933, 15 U.S. Code § 78j - Manipulative and Deceptive Devices:

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange—
>
> . . .
>
> (b)To use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, or any securities-based swap agreement any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.

186. Defendant violated Section 10(b) of the 1934 Act and Rule 10b-5 in that they: (a) employed devices, schemes, and artifices to defraud; (b) made untrue statements of material fact and/or omitted material facts necessary to make the statements not misleading; and/or (c) engaged in acts, practices, and a course of business which operated as a fraud and deceit upon Plaintiffs.

187. In addition to misrepresenting Bitcoin in its advertising, Coinbase also manipulates the Bitcoin market to generate substantial trading profits on its behalf because it operates as a "broker" and an "exchange."

188. Coinbase customers cannot "mine" Bitcoin on Coinbase's platform, which exists solely as a secondary market for Bitcoin and other cryptocurrencies.

189. When customers purchase Bitcoin through Coinbase's platform, a customer enters an order in a similar way that a broker-dealer accepts orders for stock. For example, a customer can enter a "limit" or "market" order for Bitcoin.

190. Importantly, Coinbase does not simply match buyers with sellers, like a traditional broker-dealer. Instead, Coinbase often fills customer orders by selling customers Bitcoin, which is owned by Coinbase in an internal inventory. This type of trading is known as "principal trading."

191. If Bitcoin were a stock, Coinbase would be allowed to engage in principal trading, but only as a broker-dealer with written disclosures. Brokerage firms are permitted to engage in principal trading only because their roles are limited – they cannot also act as an exchange because that would create a conflict of interest. Instead, exchanges are legally separated from brokerage firms under the Securities and Exchange Act. It has been that way for nearly 100 years.

192. This is the reason the New York Stock Exchange is prohibited from trading against its own customers. Allowing an exchange to also act as a principal would create a fundamental conflict of interest and undermine the fairness and neutrality expected in a fair market.[19]

193. Bitcoin does not trade in a fair market because Coinbase functions as both as an "exchange" and "broker" on a principal basis – this is a very dangerous conflict of interest.

194. If stock exchanges participated directly in trading it would be cheating because

[19] This would be analogous to the functions of E*Trade and the New York State Exchange being merged into one massive entity with many conflicting roles and obligations. While the notion of such a merger seems outlandish in the stock market, that is precisely how Coinbase operates and profits in the "Bitcoin Market".

the exchange would have inside information, including information about other customers' orders, which the exchange agrees to fill.

195. Coinbase cheats the Bitcoin and crypto markets because it operates as an exchange and broker. It also operates in other nefarious ways.20

196. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs suffered damages in an amount to be determined at trial, but in no event less than $20 million.

COUNT III
VIOLATION OF CALIFORNIA SECURITIES ACT

197. Plaintiffs incorporate by reference and repeat and reallege every preceding paragraph of the Complaint as if fully set forth herein.

198. The TOS between Plaintiffs and Defendant select California substantive law: "You and we agree that the laws of the State of California, without regard to principles of conflict of laws, will govern the Agreement and any Dispute, except to the extent governed by the Federal Arbitration Act or other applicable federal law."

199. Cal. Corp. Code § 25401 makes it unlawful to offer to sell a security in California by means of a communication that includes a false statement of material fact, or omits a material fact necessary to make the statement communicated not misleading.

200. California Corp. Code § 25501 provides that any person violating Section 25401 is liable to the purchaser, and "a purchaser may recover the consideration paid for the security, plus interest at the legal rate, less the amount of any income received on the security, upon the

[20] Former Coinbase Insider Sentenced In First Ever Cryptocurrency Insider Trading Case, May 9, 2023

Available here: https://www.justice.gov/usao-sdny/pr/former-coinbase-insider-sentenced-first-ever-cryptocurrency-insider-trading-case

tender of the security."

201. California's law is similar to the federal law, but with different evidentiary standards and different standards of proof for plaintiffs.

202. The acts, misrepresentation and omissions of Defendant described herein violated California's Securities Act, and Plaintiffs, as a result, are damaged and demand an amount to be proven at trial, but in no event less than $20 million.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for a judgment in favor of themselves as follows:

A. Judgment, in a monetary amount, including cryptocurrency, to be determined at trial, including compensatory damages and punitive damages against Defendant for on each of the causes of action described above;

B. Judgment, in the form of a declaration, that Bitcoin is a "security" under the Securities and Exchange Act of 1933 and 1934 and the authority established by *SEC v. Howey*;

C. Plaintiffs request a trial by jury;

D. Award Plaintiffs such other monetary damages, in the form of USD or Bitcoin, in an amount to be proven at trial, but in no event less than $20 million, for the economic injuries that it has sustained as a consequence of Defendant's actions;

E. for prejudgment interest;

F. for appropriate equitable relief;

G. for reasonable attorneys' fees and costs of investigation and litigation; and

H. for such other and further relief as the interests of law or equity may require.

Dated: New York, New York
May 16, 2025

Respectfully submitted,

MDF LAW PLLC

By: */s/ Marc Fitapelli, Esq.*
/s/Jeffrey Saxon, Esq.
28 Liberty Street, 30th Floor
New York, New York 10005
Phone: 212-203-9300
Email: marc@mdf-law.com
Jeffrey@mdf-law.com
Lead Counsel for all Plaintiffs

COIN-COUNSEL
a division of Franco LAW PLLC

By: */s/Joseph A. Franco, Esq.*
1389 Flatlands Avenue
Brooklyn, New York 11234
Phone: 646-643-4331
Email: joseph@francopllc.com
Counsel for Plaintiff Cynthia Garrett

EXHIBIT A

Satoshi - Sirius emails 2009-2011

This is the correspondence between myself (Martti Malmi, AKA Sirius) and Satoshi Nakamoto, the creator of Bitcoin.

I did not feel comfortable sharing private correspondence earlier, but decided to do so for an important trial in the UK in 2024 where I was a witness. Also, a long time has passed now since the emails were sent.

The archive is incomplete and contains only emails from my address @cc.hut.fi. My university email addresses changed to @aalto.fi in early 2011, and I don't have backups of those emails.

There are some passwords and a street address mentioned in the emails, but those are no longer valid or relevant.

Follow me on Nostr or Twitter

Font size: + -

Email #1

Date: Sat, 02 May 2009 18:06:58 +0100
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoin
To: Martti Malmi <sirius-m@users.sourceforge.net>

Thanks for starting that topic on ASC, your understanding of bitcoin is spot on. Some of their responses were rather Neanderthal, although I guess they're so used to being anti-fiat-money that anything short of gold isn't good enough. They concede that something is flammable, but argue that it'll never burn because there'll never be a spark. Once it's backed with cash, that might change, but I'd probably better refrain from mentioning that in public anymore until we're closer to ready to start. I think we'll get flooded with newbies and we need to get ready first.

What we need most right now is website writing. My writing is not that great, I'm a much better coder. Maybe you could create the website on sourceforge, which is currently blank. If you can write a FAQ, I can give you a compilation of my replies to questions in e-mail and forums for facts and details and ideas.

Codewise, there's not much that's easy right now. One thing that's needed is an interface for server side scripting languages such as Java, Python, PHP, ASP, etc. Bitcoin would be running on the web server, and server side script could call it to do transactions. It's Windows, so I guess OLE/COM is the interface.

One easy thing that really helps is to run a node that can accept incoming connections (forward port 8333 on your firewall) to make sure that new users who try it out have someone to connect to. If they run it and get no connections, they'll probably just give up.

Satoshi

Martti Malmi wrote:
> Message body follows:
>
> Hello,
>
> I'm Trickstern from the anti-state.com forum, and I would
> like to help with Bitcoin, if there's something I can do.
>
> I have a good touch on Java and C languages from school
> courses (I'm studying CS), but not so very much development
> experience yet. I think I could learn the C++ tricks quite
> easily on that basis. I could also do testing or
> documentation.
>
> Best regards,
> Martti Malmi
>
> --
> This message has been sent to you, a registered SourceForge.net user,
> by another site user, through the SourceForge.net site. This message
> has been delivered to your SourceForge.net mail alias. You may reply
> to this message using the "Reply" feature of your email client, or
> using the messaging facility of SourceForge.net at:
> https://sourceforge.net/sendmessage.php?touser=2495503
>

Email #2

Date: Sun, 03 May 2009 08:08:36 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

All right, I can do the website and the FAQ. I'll start writing the
FAQ now with the questions that I can think of.

I have a feature suggestion for the program: a UI tool for creating
password protected private keys and saving them into a custom
location. Backups of the key will be needed to be safe from losing the
control of your coins, and for using the coins on more than one
computers. Password protection would be needed to make using your
money more difficult for someone who happens to find your key file.

Maybe a bug/feature tracker could be set up at the Sourceforge project page?

I'm running a bitcoin node always when my PC is powered on, which
means about 24/7. Bitcoin is a great project, and it's really cool to
participate!

-Martti Malmi

Quoting Satoshi Nakamoto <satoshin@gmx.com>:

> Thanks for starting that topic on ASC, your understanding of bitcoin is
> spot on. Some of their responses were rather Neanderthal, although I
> guess they're so used to being anti-fiat-money that anything short of
> gold isn't good enough. They concede that something is flammable, but
> argue that it'll never burn because there'll never be a spark. Once
> it's backed with cash, that might change, but I'd probably better
> refrain from mentioning that in public anymore until we're closer to
> ready to start. I think we'll get flooded with newbies and we need to
> get ready first.
>
> What we need most right now is website writing. My writing is not that
> great, I'm a much better coder. Maybe you could create the website on
> sourceforge, which is currently blank. If you can write a FAQ, I can
> give you a compilation of my replies to questions in e-mail and forums
> for facts and details and ideas.
>
> Codewise, there's not much that's easy right now. One thing that's

> needed is an interface for server side scripting languages such as
> Java, Python, PHP, ASP, etc. Bitcoin would be running on the web
> server, and server side script could call it to do transactions. It's
> Windows, so I guess OLE/COM is the interface.
>
> One easy thing that really helps is to run a node that can accept
> incoming connections (forward port 8333 on your firewall) to make sure
> that new users who try it out have someone to connect to. If they run
> it and get no connections, they'll probably just give up.
>
> Satoshi
>
>
> Martti Malmi wrote:
>> Message body follows:
>>
>> Hello,
>>
>> I'm Trickstern from the anti-state.com forum, and I would like to
>> help with Bitcoin, if there's something I can do.
>>
>> I have a good touch on Java and C languages from school courses
>> (I'm studying CS), but not so very much development experience yet.
>> I think I could learn the C++ tricks quite easily on that basis. I
>> could also do testing or documentation.
>>
>> Best regards,
>> Martti Malmi
>>
>> --
>> This message has been sent to you, a registered SourceForge.net user,
>> by another site user, through the SourceForge.net site. This message
>> has been delivered to your SourceForge.net mail alias. You may reply
>> to this message using the "Reply" feature of your email client, or
>> using the messaging facility of SourceForge.net at:
>> https://sourceforge.net/sendmessage.php?touser=2495503
>>

Email #3

Date: Sun, 03 May 2009 23:32:26 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> All right, I can do the website and the FAQ. I'll start writing the FAQ
> now with the questions that I can think of.

That would be great! I added you (dmp1ce) as a dev to the sourceforge project and gave you access to edit the web space and everything.

> I have a feature suggestion for the program: a UI tool for creating
> password protected private keys and saving them into a custom location.
> Backups of the key will be needed to be safe from losing the control of
> your coins, and for using the coins on more than one computers. Password
> protection would be needed to make using your money more difficult for
> someone who happens to find your key file.

Definitely. This will be an absolutely essential feature once things get going, making it so you can lock your wealth up with strong encryption and back it up more securely than any physical safe. So far I've been putting it off in favour of other features because it's not crucial yet until bitcoins start to have value.

I plan to work on the escrow feature next, which is needed to make actual trades for physical stuff safer and before backing the currency with fiat money can begin.

> I'm running a bitcoin node always when my PC is powered on, which means
> about 24/7. Bitcoin is a great project, and it's really cool to
> participate!

Thanks! Right now there are a lot of people on the network who can't receive incoming connections, so every node that can really helps. Having more helps keep down the "(not accepted)" issue for now until I reduce the chances of that happening in v0.1.6.

I guess one answer for the FAQ should be how to set up your firewall to forward port 8333 so you can receive incoming connections. The question could be something like "what if I have 0 connections" and that could be

the answer that it might be because the nodes you can connect with is limited if you don't set that up.

Here's a compilation of questions I've answered in forums and e-mail that should help you see what questions are frequently asked and some answers I've used. It's not intended to use all or most of the material here, just pick and choose. This is just a dump of everything I've answered.

Some issues that we don't have easy answers for are best not to bring up. Casual users seems content to assume that the system works as stated (which it does), and getting into the design details just opens a can of worms that can't be answered without a deep understanding of the system. The advanced questions I've received have mostly been unique per person and best answered individually.

**** QUESTION AND ANSWER DUMP ****

Any questions used for the FAQ should probably be rephrased.

questions:

> The bottom of the UI shows:
>
> Generating 4 connections 4024 blocks 164 transactions
>
> I understand "generating"; I assume I am connected to 4 other nodes; and
> I know I have recorded 164 transactions (including failed generation
> attempts). I'm not clear what the "blocks" figure describes. It's much
> smaller than the total of all the blocks shown against all my transactions.
>

It's the total number of blocks in the block chain, meaning the network's block chain, which everyone has a copy of. Every Bitcoin node displays the same number and it goes up about every 10 minutes whenever someone generates a block. When you haven't had it running for a while, once you're connected it spins up rapidly as it downloads what was generated while you were gone to catch up. I'm not sure exactly how to describe it (that would fit on the status bar in 1 word, maybe 2 words max), any ideas?

The blocks number in the status column next to your transactions is the number of blocks that have come after that transaction. Your transaction is essentially "in" that many blocks.

Satoshi

> My best guess - it
> is the length of the global chain, and the rapid advance at the start
> is as the software downloads and verifies the preceding blocks in the
> chain as being valid.

Right. I'm trying to think of more clear wording for that, maybe "%d network blocks" or "%d block chain".

> I'm having an unusual run of (block not-accepted) failures, and thought I'd let you know in
> case this was of any significance.

What rate of not-accepted did you see? I didn't see anything unusual on my end. If you had more than, say, 4 in a row, that would be abnormal and probably a loss of network communication. If it's scattered and less than 25%, just random bad luck. It's normal and harmless to randomly get some per cent of not-accepted, and of course randomness can sometimes bunch up and look like a pattern.

The idea of an option to View/Hide unaccepted blocks is a good one, as well as View/Hide all generated blocks so you can more easily see incoming transactions. Seeing the unaccepted blocks is just annoying and frustrating. Everyone faces the same rate of unaccepted, it's just a part of the process. It would probably be best to default to hide unaccepted blocks, so as not to show giving and taking away something that never was, and not show new generated blocks at all until they have at least one confirmation. It would only mean finding out you have a generated block 15 minutes later than normal, and then you still have 119 blocks to go before it matures anyway. This is on the to-do list

for v0.1.6.

Satoshi

[note: I have some improvements in 0.1.6 to reduce this problem somewhat, and it'll also improve when the network is larger]

> For some reason your transfer to me shows up as "From: unknown" even
> though I added you to my address book.
>
> I have a "Generated (not accepted)" line in my transaction list, it
> seems like an attempt to generate a coin went wrong somehow. Not sure
> what happened here - presumably my node successfully solved a block
> but then I went offline before it was sent to the network?

Transactions sent to a bitcoin address will always say "from: unknown". The transaction only tells who it's to. Sending by bitcoin address has a number of problems, but it's so nice having the fallback option to be able to send to anyone whether they're online or not. There are a number of ideas to try to improve things later. For now, if things work out like the real world where the vast majority of transactions are with merchants, they'll pretty much always make sure to set up to receive by IP. The P2P file sharing networks seem fairly successful at getting a large percentage of their users to set up their firewalls to forward a port.

I badly wanted to find some way to include a comment with indirect transfers, but there just wasn't a way to do it. Bitcoin uses EC-DSA, which was essential for making the block chain compact enough to be practical with today's technology because its signatures are an order of magnitude smaller than RSA. But EC-DSA can't encrypt messages like RSA, it can only be used to verify signatures.

The "Generated (not accepted)" normally happens if two nodes find a block at close to the same time, one of them will not be accepted. It's normal and unavoidable. I plan in v0.1.6 to hide those, since they're just confusing and annoying and there's no reason for users to have to see them. While the network is still small like it is now, if you can't

receive incoming connections you're at more of a disadvantage because you can't receive block announcements as directly.

> ...So far it has two "Generated" messages, however the
> "Credit" field for those is 0.00 and the balance hasn't changed. Is
> this due to the age/maturity requirement for a coin to be valid?

Right, the credit field stays 0.00 until it matures, then it'll be 50.00. BTW, you can doubleclick on a line for details.

> ...understand correctly, there is only one (or maybe a few) global
> chain[s] into which all transactions are hashed. If there is only one
> chain recording "the story of the economy" so to speak, how does this
> scale? In an imaginary planet-wide deployment there would be millions
> of even billions of transactions per hour being hashed into the chain...

> ...I found the section on incentives hard to follow. In particular, I'm
> not clear on what triggers the transition from minting new coins as a
> reason to run a node, to charging transaction fees (isn't the point of
> BitCoin largely to zero transaction costs anyway?). Presumably there's
> some human in charge of the system...

> ...How did you decide on the inflation schedule for v1? Where did 21
> million coins come from? What denominations are these coins? You
> mention a way to combine and split value but I'm not clear on how this
> works. For instance are bitcoins always denominated by an integer or
> can you have fractional bitcoins?...

> ...it's rare that I encounter truly
> revolutionary ideas. The last time I was this excited about a new
> monetary scheme was when I discovered Ripple. If you have any thoughts
> on Ripple, I'd also love to hear them.

There is only one global chain.

The existing Visa credit card network processes about 15 million

Internet purchases per day worldwide. Bitcoin can already scale much larger than that with existing hardware for a fraction of the cost. It never really hits a scale ceiling. If you're interested, I can go over the ways it would cope with extreme size.

By Moore's Law, we can expect hardware speed to be 10 times faster in 5 years and 100 times faster in 10. Even if Bitcoin grows at crazy adoption rates, I think computer speeds will stay ahead of the number of transactions.

I don't anticipate that fees will be needed anytime soon, but if it becomes too burdensome to run a node, it is possible to run a node that only processes transactions that include a transaction fee. The owner of the node would decide the minimum fee they'll accept. Right now, such a node would get nothing, because nobody includes a fee, but if enough nodes did that, then users would get faster acceptance if they include a fee, or slower if they don't. The fee the market would settle on should be minimal. If a node requires a higher fee, that node would be passing up all transactions with lower fees. It could do more volume and probably make more money by processing as many paying transactions as it can. The transition is not controlled by some human in charge of the system though, just individuals reacting on their own to market forces.

A key aspect of Bitcoin is that the security of the network grows as the size of the network and the amount of value that needs to be protected grows. The down side is that it's vulnerable at the beginning when it's small, although the value that could be stolen should always be smaller than the amount of effort required to steal it. If someone has other motives to prove a point, they'll just be proving a point I already concede.

My choice for the number of coins and distribution schedule was an educated guess. It was a difficult choice, because once the network is going it's locked in and we're stuck with it. I wanted to pick something that would make prices similar to existing currencies, but without knowing the future, that's very hard. I ended up picking something in the middle. If Bitcoin remains a small niche, it'll be worth less per unit than existing currencies. If you imagine it being used for some fraction of world commerce, then there's only going to be 21 million coins for the whole world, so it would be worth much more per unit. Values are 64-bit integers with 8 decimal places, so 1 coin is represented internally as 100000000. There's plenty of granularity if typical prices become small. For example, if 0.001 is worth 1 Euro, then it might be easier to change where the decimal point is displayed,

so if you had 1 Bitcoin it's now displayed as 1000, and 0.001 is displayed as 1.

Ripple is interesting in that it's the only other system that does something with trust besides concentrate it into a central server.

Satoshi

> If we assume that 0.1% is a good risk rate, then z=5 thus
> any transaction must wait a bit less than an hour before being
> solidified in the chain. As micropayments for things like web content
> or virtual goods are by definition something that requires low
> overhead, waiting an hour seems like quite a significant hurdle.

For the actual risk, multiply the 0.1% by the probability that the buyer is an attacker with a huge network of computers.

For micropayments, you can safely accept the payment immediately. The size of the payment is too small for the effort to steal it. Micropayments are almost always for intellectual property, where there's no physical loss to the merchant. Anyone trying to steal a micropayment would probably not be a paying customer anyway, and if they want to steal intellectual property they can use the file sharing networks.

Currently, businesses accept a certain chargeoff rate. I believe the risk with 1 or even 0 confirming blocks will be much less than the rate of chargebacks on verified credit card transactions.

The usual scam against a merchant that doesn't wait for confirming blocks would be to send a payment to a merchant, then quickly try to propagate a double-spend to the network before the merchant's copy. What the merchant can do is broadcast his transaction and then monitor the network for any double-spend copies. The thief would not be able to broadcast during the monitoring period or else the merchant's node would receive a copy. The merchant would only have to monitor for a minute or two until most of the network nodes have his version and it's too late for the thief's version to catch up and reach many nodes. With just a minute or two delay, the chance of getting away without paying could be

made much too low to scam. A thief usually needs a high probability of getting an item for free to make it worthwhile. Using a lot of CPU power to do the brute force attack discussed in the paper in addition to the above scam would not increase the thief's chances very much.

Anything that grants access to something, like something that takes a while to download, access to a website, web hosting, a subscription or service, can be cancelled a few minutes later if the transaction is rejected.

> How is the required difficulty of each block communicated through the
> network and agreed upon?

It's not communicated. The formula is hardcoded in the program and every node does the same calculation to know what difficulty is required for the next block. If someone diverged from the formula, their block would not be accepted by the majority.

> Is the code free/open source or just open source?

It's free open source. It's the MIT license, which just requires some disclaimer text be kept with the source code, other than that you can do just about anything you want with it. The source is included in the main download.

Satoshi

> Is there a way to be told of new versions? Does the app auto update
> itself? Some kind of mailing list would be excellent.

The list is:
bitcoin-list@lists.sourceforge.net
Subscribe/unsubscribe page:
http://lists.sourceforge.net/mailman/listinfo/bitcoin-list

Archives:
http://sourceforge.net/mailarchive/forum.php?forum_name=bitcoin-list

I'll always announce new versions there. Automatic update, or at least notification of new versions, is definitely on the list.

[this inflation discussion was before the transaction fee mechanism and fixed plan of 21 million coins was posted, so it may not be as applicable anymore]

> Since they can be created for free (or at the cost
> of computer power people have anyway for other reasons),
> monetizing them means simply giving away money.

You're still thinking as if the difficulty level will be so easy that people will be able to generate all the bitcoins they want.

Imagine you have to run your computer 24/7 for a month to generate 1 cent. After a year, you could generate 12 cents. That's not going to make it so people can just generate all the bitcoin they want for spending.

The value of bitcoins would be relative to the electricity consumed to produce them. All modern CPUs save power when they're idle. If you run a computational task 24/7, not letting it idle, it uses significantly more power, and you'll notice it generates more heat. The extra wattage consumed goes straight to your power bill, and the value of the bitcoins you produce would be something less than that.

> Why would they, when they make money by generating
> new ones

No, they can't make money that way. It would cost them more in electricity than they'd be selling the bitcoins for.

Historically, people have taken up scarce commodities as money, if necessary taking up whatever is at hand, such as shells or stones. Each has a kernel of usefulness that helped bootstrap the process, but the monetary value ends up being much more than the functional value alone. Most of the value comes from the value that others place in it. Gold, for instance, is pretty, non-corrosive and easily malleable, but most of its value is clearly not from that. Brass is shiny and similar in colour. The vast majority of gold sits unused in vaults, owned by governments that could care less about its prettiness.

Until now, no scarce commodity that can be traded over a communications channel without a trusted third party has been available. If there is a desire to take up a form of money that can be traded over the Internet without a TTP, then now that is possible.

Satoshi

> As more capable
> computer hardware comes out, the natural supply per user
> doubles at every cycle of Moore's law.

Actually, that is handled. There's a moving average that compensates for the total effort being expended so that the total production is a constant. As computers get more powerful, the difficulty increases to compensate.

> I do not recall any economic history of a commodity subject
> to natural inflation ever being used as money

There's gold for one. The supply of gold increases by about 2%-3% per year. Any fiat currency typically averages more inflation than that.

> Won't there be massive inflation as computers get faster and are able to solve the proof-of-work problem faster?

The difficulty is controlled by a moving average that compensates for the total effort being expended to keep the total production constant. As computers get more powerful, the difficulty increases to compensate.

> If someone double spends, then the transaction record
> can be unblinded revealing the identity of the cheater?

Identities are not used, and there's no reliance on recourse. It's all prevention.

> ...You're saying
> there's no effort to identify and exclude nodes that don't
> cooperate? I suspect this will lead to trouble and possible DOS
> attacks.

There is no reliance on identifying anyone. As you've said, it's futile and can be trivially defeated with sock puppets.

The credential that establishes someone as real is the ability to supply CPU power.

> But in the absence of identity, there's no downside to them
> if spends become invalid, if they've already received the
> goods they double-spent for (access to website, download,
> whatever). The merchants are left holding the bag with
> "invalid" coins, unless they wait that magical "few blocks"
> (and how can they know how many?) before treating the spender
> as having paid.

> The consumers won't do this if they spend their coin and it takes
> an hour to clear before they can do what they spent their coin on.
> The merchants won't do it if there's no way to charge back a
> customer when they find the that their coin is invalid because
> the customer has doublespent.

This is a version 2 problem that I believe can be solved fairly satisfactorily for most applications.

The race is to spread your transaction on the network first. Think 6 degrees of freedom -- it spreads exponentially. It would only take something like 2 minutes for a transaction to spread widely enough that a competitor starting late would have little chance of grabbing very many nodes before the first one is overtaking the whole network. During those 2 minutes, the merchant's nodes can be watching for a double-spent transaction. The double-spender would not be able to blast his alternate transaction out to the world without the merchant getting it, so he has to wait before starting.

If the real transaction reaches 90% and the double-spent tx reaches 10%, the double-spender only gets a 10% chance of not paying, and 90% chance his money gets spent. For almost any type of goods, that's not going to be worth it for the scammer.

Information based goods like access to website or downloads are non-fencible. Nobody is going to be able to make a living off stealing access to websites or downloads. They can go to the file sharing networks to steal that. Most instant-access products aren't going to have a huge incentive to steal.

If a merchant actually has a problem with theft, they can make the customer wait 2 minutes, or wait for something in e-mail, which many already do. If they really want to optimize, and it's a large download, they could cancel the download in the middle if the transaction comes back double-spent. If it's website access, typically it wouldn't be a big deal to let the customer have access for 5 minutes and then cut off access if it's rejected. Many such sites have a free trial anyway.

Satoshi

[in response to a question about scale]

100,000 block generating nodes is a good ballpark large-scale size to think about. Propagating a transaction across the whole network twice would consume a total of US$ 0.02 of bandwidth at today's prices. In practice, many would be burning off excess allocated bandwidth or unlimited plans with one of the cheaper backbones. There could be millions of SPV clients. They only matter in how many transactions they generate. If they pay 1 or 2 cents transaction fees, they pay for themselves. I've coded it so you can pay any optional amount of transaction fees you want. When the incentive subsidy eventually tapers off, it may be necessary to put a market-determined transaction fee on your transactions to make sure nodes process them promptly.

To think about what a really huge transaction load would look like, I look at the existing credit card network. I found some more estimates about how many transactions are online purchases. It's about 15 million tx per day for the entire e-commerce load of the Internet worldwide. At 1KB per transaction, that would be 15GB of bandwidth for each block generating node per day, or about two DVD movies worth. Seems do-able even with today's technology.

Important to remember, even if Bitcoin caught on at dot-com rates of growth, it would still take years to become any substantial fraction of all transactions. I believe hardware has already recently become strong enough to handle large scale, but if there's any doubt about that, bandwidth speeds, prices, disk space and computing power will be much greater by the time it's needed.

Satoshi

> One other question I had... What prevents the single node with the most
> CPU power from generating and retaining the majority of the BitCoins?

> If every node is working independently of all others, if one is
> significantly more powerful than the others, isn't it probable that this
> node will reach the proper conclusion before other nodes? An
> underpowered node may get lucky once in a while, but if they are at a
> significant horsepower advantage I would expect the majority of BitCoins
> to be generated by the most powerful node.

It's not like a race where if one car is twice as fast, it'll always win. It's an SHA-256 that takes less than a microsecond, and each guess has an independent chance of success. Each computer's chance of finding a hash collision is linearly proportional to it's CPU power. A computer that's half as fast would get half as many coins.

[question about what to backup]

The files are in "%appdata%\Bitcoin", that's the directory to backup.

%appdata% is per-user access privilege. Most new programs like Firefox store their settings files there, despite the headwind of Microsoft changing the directory name with every Windows release and being full of spaces and so long it runs off the screen.

[question about what to backup]

The directory is "%appdata%\Bitcoin"
It has spaces in it so you need the quotes
cd "%appdata%\bitcoin"

On XP it would typically be:
C:\Documents and Settings\[username]\Application Data\Bitcoin

Backup that whole directory. All data files are in that directory. There are no temporary files.

[question about what to backup]

The crucial file to backup is wallet.dat. If bitcoin is running then you have to backup the whole %appdata%\bitcoin directory including the database subdirectory, but even if it's not running it certainly feels safer to always backup the whole directory.

The database unfortunately names its files "log.0000000001". To the rest of the world, "log" means delete-at-will, but to database people it means delete-and-lose-everything-in-your-other-files. I tried to put them out of harm's way by putting them in the database subdirectory. Later I'll write code to flush the logs after every wallet change so wallet.dat will be standalone safe almost all the time.

> > You know, I think there were a lot more people interested in the 90's,
> > but after more than a decade of failed Trusted Third Party based systems
> > (Digicash, etc), they see it as a lost cause. I hope they can make the
> > distinction that this is the first time I know of that we're trying a
> > non-trust-based system.
>
> Yea, that was the primary feature that caught my eye. The real trick
> will be to get people to actually value the Bitcoins so that they become
> currency.

Hal sort of alluded to the possibility that it could be seen as a long-odds investment. I would be surprised if 10 years from now we're not using electronic currency in some way, now that we know a way to do it that won't inevitably get dumbed down when the trusted third party gets cold feet.

Once it gets bootstrapped, there are so many applications if you could effortlessly pay a few cents to a website as easily as dropping coins in a vending machine.

[this next bit turned out to be very controversial. there is extreme prejudice against spam solutions, especially proof-of-work.]

It can already be used for pay-to-send e-mail. The send dialog is resizeable and you can enter as long of a message as you like. It's sent directly when it connects. The recipient doubleclicks on the transaction to see the full message. If someone famous is getting more e-mail than they can read, but would still like to have a way for fans to contact them, they could set up Bitcoin and give out the IP address on their website. "Send X bitcoins to my priority hotline at this IP and I'll read the message personally."

Subscription sites that need some extra proof-of-work for their free trial so it doesn't cannibalize subscriptions could charge bitcoins for the trial.

[again, I don't know why I'm including this, as it's best to stay away from claims about spam. people automatically react violently against any suggestion of a spam solution.]

> Spammer botnets could burn through pay-per-send email filters
> trivially (as usual, the costs would fall on people other than the
> botnet herders & spammers).

Then you could earn a nice profit by setting up pay-per-send e-mail addresses and collecting all the spam money. You could sell it back to spammers who don't have big enough botnets to generate their own, helping bootstrap the currency's value. As more people catch on, they'll set up more and more phony addresses to harvest it. By the time the book "How I got rich exploiting spammers and you can too" is coming out, there'll be too many fake addresses and the spammers will have to give up.

> > * Spammer botnets could burn through pay-per-send email filters
> > trivially
> If POW tokens do become useful, and especially if they become money,
> machines will no longer sit idle. Users will expect their computers to
> be earning them money (assuming the reward is greater than the cost to
> operate). A computer whose earnings are being stolen by a botnet will
> be more noticeable to its owner than is the case today, hence we might
> expect that in that world, users will work harder to maintain their
> computers and clean them of botnet infestations.

One more factor that would mitigate spam if POW tokens have value: there would be a profit motive for people to set up massive quantities of fake e-mail accounts to harvest POW tokens from spam. They'd essentially be reverse-spamming the spammers with automated mailboxes that collect their POW and don't read the message. The ratio of fake mailboxes to real people could become too high for spam to be cost effective.

The process has the potential to establish the POW token's value in the first place, since spammers that don't have a botnet could buy tokens from harvesters. While the buying back would temporarily let more spam through, it would only hasten the self-defeating cycle leading to too many harvesters exploiting the spammers.

Interestingly, one of the e-gold systems already has a form of spam called "dusting". Spammers send a tiny amount of gold dust in order to put a spam message in the transaction's comment field. If the system let users configure the minimum payment they're willing to receive, or at least the minimum that can have a message with it, users could set how much they're willing to get paid to receive spam.

> The last thing we need is to deploy a system designed to burn all
> available cycles, consuming electricity and generating carbon dioxide,
> all over the Internet, in order to produce small amounts of bitbux to
> get emails or spams through.
>
> Can't we just convert actual money in a bank account into bitbux --

> cheaply and without a carbon tax? Please?

Ironic if we end up having to choose between economic liberty and conservation.

Unfortunately, proof of work is the only solution I've found to make p2p e-cash work without a trusted third party. Even if I wasn't using it secondarily as a way to allocate the initial distribution of currency, PoW is fundamental to coordinating the network and preventing double-spending.

If it did grow to consume significant energy, I think it would still be less wasteful than the labour and resource intensive conventional banking activity it would replace. The cost would be an order of magnitude less than the billions in banking fees that pay for all those brick and mortar buildings, skyscrapers and junk mail credit card offers.

Satoshi

> BTW I don't remember if we talked about this, but the other day some
> people were mentioning secure timestamping. You want to be able to
> prove that a certain document existed at a certain time in the past.
> Seems to me that bitcoin's stack of blocks would be perfect for this.

Indeed, Bitcoin is a distributed secure timestamp server for transactions. A few lines of code could create a transaction with an extra hash in it of anything that needs to be timestamped.
I should add a command to timestamp a file that way.

From a thread on p2presearch which starts with my rant about trust being the root weakness of all conventional financial systems.
http://listcultures.org/pipermail/p2presearch_listcultures.org/2009-February/thread.html

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what.

It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.

One of the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big problem unsolved: double-spending. Any owner could try to re-spend an already spent coin by signing it again to another owner. The usual solution is for a trusted company with a central database to check for double-spending, but that just gets back to the trust model. In its central position, the company can override the users, and the fees needed to support the company make micropayments impractical.

Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle. For details on how it works, see the design paper at http://www.bitcoin.org/bitcoin.pdf

The result is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending.

Satoshi Nakamoto
http://www.bitcoin.org

Martien van Steenbergen Martien at AardRock.COM
Thu Feb 12 08:40:53 CET 2009

Very interesting. Is this akin to David Chaum's anonymous digital money? His concept makes sure money is anonymous unless it is compromised, i.e. the same money spent more than once. As soon as it's compromised, the ‘counterfeiter’ is immediately publicly exposed.

Also, in bitcoin, is there a limited supply of money (that must be managed)? Or is money created exaclty at the moment of transaction?

Succes en plezier,

Martien.

Martien van Steenbergen wrote:
> Very interesting. Is this akin to David Chaum's anonymous digital money?
> His concept makes sure money is anonymous unless it is compromised, i.e.
> the same money spent more than once. As soon as it's compromised, the
> ‘counterfeiter’ is immediately publicly exposed.

It's similar in that it uses digital signatures for coins, but different in the approach to privacy and preventing double-spending. The recipient of a Bitcoin payment is able to check whether it is the first spend or not, and second-spends are not accepted. There isn't an off-line mode where double-spenders are caught and shamed after the fact, because that would require participants to have identities.

To protect privacy, key pairs are used only once, with a new one for every transaction. The owner of a coin is just whoever has its private key.

Of course, the biggest difference is the lack of a central server. That was the Achilles heel of Chaumian systems; when the central company shut down, so did the currency.

> Also, in bitcoin, is there a limited supply of money (that must be
> managed)? Or is money created exaclty at the moment of transaction?

There is a limited supply of money. Circulation will be 21,000,000 coins. Transactions only transfer ownership.

Thank you for your questions,

Satoshi

Martien van Steenbergen wrote:
> Reminds me of:
>
> * AardRock » Wizard Rabbit Treasurer
> <http://wiki.aardrock.com/Wizard_Rabbit_Treasurer>; and
> * AardRock » Pekunio <http://wiki.aardrock.com/Pekunio>

Indeed, it is much like Pekunio in the concept of spraying redundant copies of every transaction to a number of peers on the network, but the implementation is not a reputation network like Wizard Rabbit Treasurer.
In fact, Bitcoin does not use reputation at all. It sees the network as just a big crowd and doesn't much care who it talks to or who tells it something, as long as at least one of them relays the information being broadcast around the network. It doesn't care because there's no

way to lie to it. Either you tell it crypto proof of something, or it ignores you.

> Are you familiar with Ripple?

As trust systems go, Ripple is unique in spreading trust around rather than concentrating it.

[I've been asked at least 4 other times "have you heard of Ripple?"]

Michel Bauwens wrote:
> how operational is your project? how soon do you think people will be
> able to use it in real life?

It's fully operational and the network is growing. If you try the software, e-mail me your Bitcoin address and I'll send you a few coins.

We just need to spread the word and keep getting more people interested.

Here's a link to the original introduction of the paper on the Cryptography mailing list. (Inflation issues were superseded by changes I made later to support transaction fees and the limited circulation plan. This link is a moving target, this archive page is just a certain number of days back and the discussion will keep scrolling off to the next page.)
http://www.mail-archive.com/cryptography@metzdowd.com/mail3.html

A little follow up when the software was released.
http://www.mail-archive.com/cryptography@metzdowd.com/mail2.html

My description of how Bitcoin solves the Byzantine Generals' problem:
http://www.bitcoin.org/byzantine.html

Email #4

Date: Mon, 04 May 2009 03:17:22 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Quoting Satoshi Nakamoto <satoshin@gmx.com>:

> That would be great! I added you (dmp1ce) as a dev to the sourceforge
> project and gave you access to edit the web space and everything.

Oh, that's not me but another guy who wanted to help. I've seen him on
the Freedomain Radio forum. My name is Martti Malmi and my Sourceforge
account is sirius-m. No problem!

Thanks for your answered questions, I'll add them to the faq. Here's
what I've done so far:

**** Bitcoin FAQ ****

General Questions

1 What is bitcoin?

Bitcoin is a peer-to-peer network based anonymous digital
currency. Peer-to-peer (P2P) means that there is no central
authority to issue new money or to keep track of the
transactions. Instead, those tasks are managed collectively by
the nodes of the network. Anonymity means that the real world
identity of the parties of a transaction can be kept hidden from
the public or even from the parties themselves.

2 How does bitcoin work?

Bitcoin utilizes public/private key cryptography. When a coin is
transfered from user A to user B, A adds B's public key to the
coin and signs it with his own private key. Now B owns the coin
and can transfer it further. To prevent A from transfering the
already used coin to another user C, a public list of all the
previous transactions is collectively maintained by the network
of bitcoin nodes, and before each transaction the coin's
unusedness will be checked.

For details, see chapter Advanced Questions.

3 What is bitcoin's value backed by?

Bitcoin is valued for the things it can be exchanged to, just like all the traditional paper currencies are.

When the first user publicly announces that he will make a pizza for anyone who gives him a hundred bitcoins, then he can use bitcoins as payment to some extent - as much as people want pizza and trust his announcement. A pizza-eating hairdresser who trusts him as a friend might then announce that she starts accepting bitcoins as payment for fancy haircuts, and the value of the bitcoin would be higher - now you could buy pizzas and haircuts with them. When bitcoins have become accepted widely enough, he could retire from his pizza business and still be able to use his bitcoin-savings.

4 How are new bitcoins created?

New coins are generated by a network node each time it finds the solution to a certain calculational problem. In the first 4 years of the bitcoin network, amount X of coins will be created. The amount is halved each 4 years, so it will be X/2 after 4 years, X/4 after 8 years and so on. Thus the total number of coins will approach 2X.

5 Is bitcoin safe?

Yes, as long as you make backups of your coin keys, protect them with strong passwords and keep keyloggers away from your computer. If you lose your key or if some unknown attacker manages to unlock it, there's no way to get your coins back. If you have a large amount of coins, it is recommended to distribute them under several keys. You propably wouldn't either keep all your dollars or euros as paper in a single wallet and leave it unguarded.

6 Why should I use bitcoin?

- Transfer money easily through the internet, without having to trust third parties.

- Third parties can't prevent or control your transactions.

- Be safe from the unfair monetary policies of the monopolistic central banks and the other risks of centralized power over a money supply. The limited inflation of the bitcoin system's money supply is distributed evenly (by CPU power) throughout the network, not monopolized to a banking elite.

- Bitcoin's value is likely to increase as the growth of the bitcoin economy exceeds the inflation rate - consider bitcoin an investment and start running a node today!

7 Where can I get bitcoins?

Find a bitcoin owner and sell her something - MMORPG equipement, IT support, lawn mowing, dollars or whatever you can trade with her. You can also generate new bitcoins for yourself by running a bitcoin network node.

Email #5

Date: Mon, 04 May 2009 16:51:00 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

Oh crap, I got your sourceforge usernames mixed up, sorry about that. I clicked on the wrong e-mail when I was looking for your username. You now have access.

Your FAQ looks good so far!

You can create whatever you want on bitcoin.sourceforge.net. Something to get new users up to speed on what Bitcoin is and how to use it and why, and clean and professional looking would help make it look well established. The site at bitcoin.org was designed in a more professorial style when I was presenting the design paper on the Cryptography list, but we're moving on from that phase.

You should probably change the part about "distribute them under several keys". When the paper says that it means for the software to do it, and it does. For privacy reasons, the software already uses a different key for every transaction, so every piece of money in your wallet is already

on a different key. The exception is when using a bitcoin address, everything sent to the same bitcoin address is on the same key, which is a privacy risk if you're trying to be anonymous. The EC-DSA key size is very strong (sized for the future), we don't practically have to worry about a key getting broken, but if we did there's the advantage that someone expending the massive computing resources would only break one single transaction's worth of money, not someone's whole account. The details about how to backup your wallet files is in the Q&A dump and also it's explained in readme.txt and definitely belongs in the FAQ.

Oh I see, you're trying to address byronm's concern on freedomainradio. I see what you mean about the password feature being useful to address that argument. Banks let anyone who has your name and account number drain your account, and you're not going to get it back from Nigeria. If someone installs a keylogger on your computer, they could just as easily get your bank password and transfer money out of your account. Once we password encrypt the wallet, we'll be able to make a clearer case that we're much more secure than banks. We use strong encryption, while banks still let anyone who has your account info draw money from your account.

mmalmi@cc.hut.fi wrote:
> Quoting Satoshi Nakamoto <satoshin@gmx.com>:
>
>> That would be great! I added you (dmp1ce) as a dev to the sourceforge
>> project and gave you access to edit the web space and everything.
>
> Oh, that's not me but another guy who wanted to help. I've seen him on
> the Freedomain Radio forum. My name is Martti Malmi and my Sourceforge
> account is sirius-m. No problem!
>
> Thanks for your answered questions, I'll add them to the faq. Here's
> what I've done so far:
>
> **** Bitcoin FAQ ****
>
> General Questions
>
> 1 What is bitcoin?
>
> Bitcoin is a peer-to-peer network based anonymous digital
> currency. Peer-to-peer (P2P) means that there is no central

> authority to issue new money or to keep track of the
> transactions. Instead, those tasks are managed collectively by
> the nodes of the network. Anonymity means that the real world
> identity of the parties of a transaction can be kept hidden from
> the public or even from the parties themselves.
>
> 2 How does bitcoin work?
>
> Bitcoin utilizes public/private key cryptography. When a coin is
> transfered from user A to user B, A adds B's public key to the
> coin and signs it with his own private key. Now B owns the coin
> and can transfer it further. To prevent A from transfering the
> already used coin to another user C, a public list of all the
> previous transactions is collectively maintained by the network
> of bitcoin nodes, and before each transaction the coin's
> unusedness will be checked.
>
> For details, see chapter Advanced Questions.
>
> 3 What is bitcoin's value backed by?
>
> Bitcoin is valued for the things it can be exchanged to, just
> like all the traditional paper currencies are.
>
> When the first user publicly announces that he will make a pizza
> for anyone who gives him a hundred bitcoins, then he can use
> bitcoins as payment to some extent - as much as people want pizza
> and trust his announcement. A pizza-eating hairdresser who trusts
> him as a friend might then announce that she starts accepting
> bitcoins as payment for fancy haircuts, and the value of the
> bitcoin would be higher - now you could buy pizzas and haircuts
> with them. When bitcoins have become accepted widely enough, he
> could retire from his pizza business and still be able to use his
> bitcoin-savings.
>
> 4 How are new bitcoins created?
>
> New coins are generated by a network node each time it finds the
> solution to a certain calculational problem. In the first 4 years
> of the bitcoin network, amount X of coins will be created. The
> amount is halved each 4 years, so it will be X/2 after 4 years,
> X/4 after 8 years and so on. Thus the total number of coins will
> approach 2X.

> 5 Is bitcoin safe?
>
> Yes, as long as you make backups of your coin keys, protect them with strong passwords and keep keyloggers away from your computer. If you lose your key or if some unknown attacker manages to unlock it, there's no way to get your coins back. If you have a large amount of coins, it is recommended to distribute them under several keys. You propably wouldn't either keep all your dollars or euros as paper in a single wallet and leave it unguarded.
>
> 6 Why should I use bitcoin?
>
> • Transfer money easily through the internet, without having to trust third parties.
>
> • Third parties can't prevent or control your transactions.
>
> • Be safe from the unfair monetary policies of the monopolistic central banks and the other risks of centralized power over a money supply. The limited inflation of the bitcoin system's money supply is distributed evenly (by CPU power) throughout the network, not monopolized to a banking elite.
>
> • Bitcoin's value is likely to increase as the growth of the bitcoin economy exceeds the inflation rate - consider bitcoin an investment and start running a node today!
>
> 7 Where can I get bitcoins?
>
> Find a bitcoin owner and sell her something - MMORPG equipement, IT support, lawn mowing, dollars or whatever you can trade with her. You can also generate new bitcoins for yourself by running a bitcoin network node.
>

Email #6

Date: Tue, 05 May 2009 04:00:00 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Quoting Satoshi Nakamoto <satoshin@gmx.com>:

> You can create whatever you want on bitcoin.sourceforge.net. Something
> to get new users up to speed on what Bitcoin is and how to use it and
> why, and clean and professional looking would help make it look well
> established. The site at bitcoin.org was designed in a more
> professorial style when I was presenting the design paper on the
> Cryptography list, but we're moving on from that phase.

Ok. Could you set the project MySQL database passwords so that I can
set up a CMS on the site? I was thinking about WordPress, as it seems
simple and well maintained. I need a password for the read/write
account and one database (or the database admin pass to create it
myself). This can be done somewhere in the project admin pages, I think.

> You should probably change the part about "distribute them under
> several keys". When the paper says that it means for the software to
> do it, and it does. For privacy reasons, the software already uses a
> different key for every transaction, so every piece of money in your
> wallet is already on a different key. The exception is when using a
> bitcoin address, everything sent to the same bitcoin address is on the
> same key, which is a privacy risk if you're trying to be anonymous.
> The EC-DSA key size is very strong (sized for the future), we don't
> practically have to worry about a key getting broken, but if we did
> there's the advantage that someone expending the massive computing
> resources would only break one single transaction's worth of money, not
> someone's whole account. The details about how to backup your wallet
> files is in the Q&A dump and also it's explained in readme.txt and
> definitely belongs in the FAQ.

Ok, that's good to know.

> Oh I see, you're trying to address byronm's concern on freedomainradio.
> I see what you mean about the password feature being useful to address
> that argument. Banks let anyone who has your name and account number
> drain your account, and you're not going to get it back from Nigeria.
> If someone installs a keylogger on your computer, they could just as
> easily get your bank password and transfer money out of your account.
> Once we password encrypt the wallet, we'll be able to make a clearer
> case that we're much more secure than banks. We use strong encryption,
> while banks still let anyone who has your account info draw money from
> your account.

Well, I guess that's true after all.

Email #7

Date: Tue, 05 May 2009 04:07:41 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Quoting mmalmi@cc.hut.fi:

>> Oh I see, you're trying to address byronm's concern on freedomainradio.
>> I see what you mean about the password feature being useful to address
>> that argument. Banks let anyone who has your name and account number
>> drain your account, and you're not going to get it back from Nigeria.
>> If someone installs a keylogger on your computer, they could just as
>> easily get your bank password and transfer money out of your account.
>> Once we password encrypt the wallet, we'll be able to make a clearer
>> case that we're much more secure than banks. We use strong encryption,
>> while banks still let anyone who has your account info draw money from
>> your account.
>
> Well, I guess that's true after all.

...the difference being, though, that not everyone can easily transfer
their regular bank money into an uncontrollable location. In bitcoin
anyone can do it.

Email #8

Date: Tue, 05 May 2009 18:39:44 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
>> You can create whatever you want on bitcoin.sourceforge.net. Something
>> to get new users up to speed on what Bitcoin is and how to use it and
>> why, and clean and professional looking would help make it look well

>> established. The site at bitcoin.org was designed in a more
>> professorial style when I was presenting the design paper on the
>> Cryptography list, but we're moving on from that phase.
>
> Ok. Could you set the project MySQL database passwords so that I can set
> up a CMS on the site? I was thinking about WordPress, as it seems simple
> and well maintained. I need a password for the read/write account and
> one database (or the database admin pass to create it myself). This can
> be done somewhere in the project admin pages, I think.

They have Wordpress built in, you might not need to set up any database stuff manually. I enabled the Wordpress feature and added you as an admin, account sirius-m, e-mail sirius-m@users.sourceforge.net. I'm not sure how it works out the password for access, maybe it's just based on being logged in to sourceforge.

https://apps.sourceforge.net/wordpress/bitcoin/wp-admin/

They also have support for MediaWiki if you want it.

In case you still need it, here's the accounts and passwords for mysql.

Access this project's databases over the Internet
https://apps.sourceforge.net/admin/Bitcoin
Documentation: Guide to MySQL Database Services
http://p.sf.net/sourceforge/mysql
Hostname: mysql-b   (exactly as shown, with no domain suffix)
Database name prefix: b244765_ -- i.e. "CREATE DATABASE b244765_myapp"
as your ADMIN user.
RO user: b244765ro (SELECT)
RW user: b244765rw (SELECT, INSERT, DELETE, UPDATE)
ADMIN user: b244765admin (has RW account privileges, and CREATE, DROP,
ALTER, INDEX, LOCK TABLES)
web-access URL: https://mysql-b.sourceforge.net/
passwords:
b244765ro   EaG3nHLL
b244765rw   sNKgyt4W
b244765admin   Mz589ZKf

> ...the difference being, though, that not everyone can easily
> transfer their regular bank money into an uncontrollable location. In
> bitcoin anyone can do it.

That's true.

We shouldn't try to use security against identity theft as a selling point, since it leads into these counter arguments. The current banking model is already tested and the actual loss percentage is known. Even if ours is probably better, it's an unknown, so people can imagine anything. The uncertainty about what the average loss percentage will be is greater than the likely loss percentage itself.

Email #9

Date: Wed, 06 May 2009 08:31:41 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Quoting Satoshi Nakamoto <satoshin@gmx.com>:

> They have Wordpress built in, you might not need to set up any database
> stuff manually.
>
> They also have support for MediaWiki if you want it.

The built-in Wordpress comes with ads, and new plugins and themes need to be installed by the Sourceforge staff, so I installed Wordpress at http://bitcoin.sourceforge.net/. The admin page is at .../wp-admin/, with admin/Wubreches3eS as login. If there's something to add or change, feel free to.

The current layout is just a quickly applied free theme, but I'll see if I can do something more visual myself.

The MediaWiki might be quite useful for maintaining the FAQ, which could be retrieved from there to the main site somehow. The wiki says I need to be an editor or admin to create a new page, which is funny, because
https://apps.sourceforge.net/mediawiki/bitcoin/index.php?title=Special:ListGroupRights says that users can create
pages.

Email #10

Date: Wed, 06 May 2009 08:41:43 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Lainaus mmalmi@cc.hut.fi:

> The current layout is just a quickly applied free theme, but I'll see
> if I can do something more visual myself.

And of course I'll continue improving the contents also.

Email #11

Date: Thu, 07 May 2009 03:35:50 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

It's already an improvement, and like you say, there must be better
themes to choose from.

It would be good to make the download link go directly to the download area:
https://sourceforge.net/project/showfiles.php?group_id=244765

I haven't found any way to gain admin control over the mediawiki
feature. It thinks I'm a different S_nakamoto from the one that has
admin access:

    User list
    * S nakamoto <- it thinks I'm this one
    * S nakamoto (admin, editor)
    * Sirius-m

I tried deleting and re-enabling the feature, no help. Oh well.

mmalmi@cc.hut.fi wrote:
> Quoting Satoshi Nakamoto <satoshin@gmx.com>:
>
>> They have Wordpress built in, you might not need to set up any database

>> stuff manually.
>>
>> They also have support for MediaWiki if you want it.
>
> The built-in Wordpress comes with ads, and new plugins and themes need
> to be installed by the Sourceforge staff, so I installed Wordpress at
> http://bitcoin.sourceforge.net/. The admin page is at .../wp-admin/,
> with admin/Wubreches3eS as login. If there's something to add or change,
> feel free to.
>
> The current layout is just a quickly applied free theme, but I'll see if
> I can do something more visual myself.
>
> The MediaWiki might be quite useful for maintaining the FAQ, which could
> be retrieved from there to the main site somehow. The wiki says I need
> to be an editor or admin to create a new page, which is funny, because
> https://apps.sourceforge.net/mediawiki/bitcoin/index.php?title=Special:ListGroupRights
> says that users can create pages.

Email #12

Date: Fri, 22 May 2009 11:05:56 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Quoting Satoshi Nakamoto <satoshin@gmx.com>:

> I haven't found any way to gain admin control over the mediawiki
> feature. It thinks I'm a different S_nakamoto from the one that has
> admin access:
>   User list
>   * S nakamoto <- it thinks I'm this one
>   * S nakamoto (admin, editor)
>   * Sirius-m
>
> I tried deleting and re-enabling the feature, no help. Oh well.

I think this has something to do with the underscore character in your
username; MediaWiki handles them as spaces. I could ask SF Support

about this.

Email #13

Date: Fri, 22 May 2009 11:08:43 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Quoting mmalmi@cc.hut.fi:

> Quoting Satoshi Nakamoto <satoshin@gmx.com>:
>
>> I haven't found any way to gain admin control over the mediawiki
>> feature. It thinks I'm a different S_nakamoto from the one that has
>> admin access:
>>   User list
>>   * S nakamoto <- it thinks I'm this one
>>   * S nakamoto (admin, editor)
>>   * Sirius-m
>>
>> I tried deleting and re-enabling the feature, no help. Oh well.
>
> I think this has something to do with the underscore character in your
> username; MediaWiki handles them as spaces. I could ask SF Support
> about this.

Or could you control the MediaWiki with your account nakamoto2?

Email #14

Date: Fri, 22 May 2009 11:12:41 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Quoting mmalmi@cc.hut.fi:

> Quoting mmalmi@cc.hut.fi:

>
>> Quoting Satoshi Nakamoto <satoshin@gmx.com>:
>>
>>> I haven't found any way to gain admin control over the mediawiki
>>> feature. It thinks I'm a different S_nakamoto from the one that has
>>> admin access:
>>>   User list
>>>   * S nakamoto <- it thinks I'm this one
>>>   * S nakamoto (admin, editor)
>>>   * Sirius-m
>>>
>>> I tried deleting and re-enabling the feature, no help. Oh well.
>>
>> I think this has something to do with the underscore character in your
>> username; MediaWiki handles them as spaces. I could ask SF Support
>> about this.
>
> Or could you control the MediaWiki with your account nakamoto2?

Oh, sorry for spamming with emails, but the problem is indeed with the
underscore character:
http://apps.sourceforge.net/trac/sourceforge/ticket/300

Email #15

Date: Sun, 24 May 2009 23:03:38 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

You're right, that was it. I went in and granted us access using the
alternate account.

I like your idea of at least moving the FAQ into the wiki. I've seen
other projects that use the wiki for the FAQ or even the whole site. If
you can figure out how to make it so regular users can edit things, then
anyone who wants to can help.

mmalmi@cc.hut.fi wrote:
> Quoting mmalmi@cc.hut.fi:
>
>> Quoting mmalmi@cc.hut.fi:

>>
>>> Quoting Satoshi Nakamoto <satoshin@gmx.com>:
>>>
>>>> I haven't found any way to gain admin control over the mediawiki
>>>> feature. It thinks I'm a different S_nakamoto from the one that has
>>>> admin access:
>>>>   User list
>>>>   * S nakamoto <- it thinks I'm this one
>>>>   * S nakamoto (admin, editor)
>>>>   * Sirius-m
>>>>
>>>> I tried deleting and re-enabling the feature, no help. Oh well.
>>>
>>> I think this has something to do with the underscore character in your
>>> username; MediaWiki handles them as spaces. I could ask SF Support
>>> about this.
>>
>> Or could you control the MediaWiki with your account nakamoto2?
>
> Oh, sorry for spamming with emails, but the problem is indeed with the
> underscore character:
> http://apps.sourceforge.net/trac/sourceforge/ticket/300
>

Email #16

Date: Sun, 07 Jun 2009 08:34:29 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

> I like your idea of at least moving the FAQ into the wiki. I've seen
> other projects that use the wiki for the FAQ or even the whole site.
> If you can figure out how to make it so regular users can edit things,
> then anyone who wants to can help.

The user group privileges seemingly can't be changed without changing
the wiki source files, which can only be done by the SF admins as a
hosted app is concerned. The hosted apps are also otherwise quite
inflexible: you can only login with a SF account, you can't change
themes by yourself and of course there's the ad-bar above the pages.

I think that replacing the current Wordpress installation at bitcoin.sourceforge.net with TikiWiki could be a great solution. TikiWiki supports CMS features, forums, wikis, bug trackers, and many other features also if needed. Perhaps the best looking example of a TikiWiki installation is at http://support.mozilla.com/.

I'll take backup of the current site and see if TikiWiki can be installed at SF. If it doesn't work, I'll see how wiki/forum features can be integrated with Wordpress or think of something else.

Email #17

Date: Tue, 09 Jun 2009 09:55:26 +0300
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoin

I couldn't get TikiWiki to work, so I installed Bitweaver, which is a lightweight TikiWiki derivative. Its functionality looks good for the purpose and it's easy to customize.

The admin account password is Wubreches3eS again. New users can register to the site and write to the wiki and the forums. Next I'm going to look into how custom menus and custom layouts are made.

Email #18

Date: Thu, 11 Jun 2009 07:34:20 +0300
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoin

Now that the project web is up and running, do you think that setting up a custom VHOST for the bitcoin.org domain would be a good idea? Instructions:
http://apps.sourceforge.net/trac/sourceforge/wiki/Custom%20VHOSTs

Also, could you please send me a link to a SF Logo for statistics, as instructed at:
http://apps.sourceforge.net/trac/sourceforge/wiki/Use%20of%20sflogo%20for%20statistics%20tr

acking

Email #19

Date: Thu, 11 Jun 2009 22:24:25 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

The site layout is looking nicer. More impressive looking.

There are a lot of things you can say on the sourceforge site that I
can't say on my own site. Even so, I'm uncomfortable with explicitly
saying "consider it an investment". That's a dangerous thing to say and
you should delete that bullet point. It's OK if they come to that
conclusion on their own, but we can't pitch it as that.

A few details: the FAQ says "see section 2.3", but the sections aren't
numbered. Also, could you delete the last sentence on the FAQ "They are
planned to be hidden in v0.1.6, since they're just confusing and
annoying and there's no reason for users to have to see them." -- that's
not really something I meant to say publicly.

The links to sites to help set up 8333 port forwarding is great.
favicon is a nice touch.

Someone came up with the word "cryptocurrency"... maybe it's a word we
should use when describing Bitcoin, do you like it?

Sourceforge is so slow right now I can't even get the login page to
load. Maybe due to the site reorg they just did. I'll keep trying and
try to get you that logo stats thing.

mmalmi@cc.hut.fi wrote:
> Now that the project web is up and running, do you think that setting up
> a custom VHOST for the bitcoin.org domain would be a good idea?
> Instructions:
> http://apps.sourceforge.net/trac/sourceforge/wiki/Custom%20VHOSTs
>
> Also, could you please send me a link to a SF Logo for statistics, as
> instructed at:
>

http://apps.sourceforge.net/trac/sourceforge/wiki/Use%20of%20sflogo%20for%20statistics%20tracking
>
>

Email #20

Date: Fri, 12 Jun 2009 12:22:34 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

> There are a lot of things you can say on the sourceforge site that I
> can't say on my own site. Even so, I'm uncomfortable with explicitly
> saying "consider it an investment". That's a dangerous thing to say
> and you should delete that bullet point. It's OK if they come to that
> conclusion on their own, but we can't pitch it as that.
>
> A few details: the FAQ says "see section 2.3", but the sections aren't
> numbered. Also, could you delete the last sentence on the FAQ "They
> are planned to be hidden in v0.1.6, since they're just confusing and
> annoying and there's no reason for users to have to see them." --
> that's not really something I meant to say publicly.

I made the changes. You could also register to the site or use the admin account to make necessary changes yourself, since the pages are located in the wiki.

> Someone came up with the word "cryptocurrency"... maybe it's a word we
> should use when describing Bitcoin, do you like it?

It sounds good. "The P2P Cryptocurrency" could be considered as the slogan, even if it's a bit more difficult to say than "The Digital P2P Cash". It still describes the system better and sounds more interesting, I think.

I could notify the mailing list about the new site and invite them to write on the forums and to the wiki.

Email #21

Date: Sun, 14 Jun 2009 21:30:58 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> I made the changes. You could also register to the site or use the admin
> account to make necessary changes yourself, since the pages are located
> in the wiki.

Thanks, I've been really busy lately.

I registered username "satoshi". Since there's no SSL login, I want to mainly use that account with sub-admin powers and use the admin account as little as possible. I created a "Moderators" group to give my satoshi account as much editing control as possible without the ability to overthrow everything.

There's something weird with the download bar on the right covering things up, like on the new account registration it covers up the entry fields unless you make the browser really wide, and the homepage it covers up the screenshots. (with Firefox)

Email #22

Date: Mon, 22 Jun 2009 19:27:11 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

> There's something weird with the download bar on the right covering
> things up, like on the new account registration it covers up the entry
> fields unless you make the browser really wide, and the homepage it
> covers up the screenshots. (with Firefox)

Problem fixed. I switched to a fixed width layout, which is also easier to read as the lines are shorter.

Email #23

Date: Tue, 21 Jul 2009 03:43:34 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Hi,

I made a post on the Bitcoin developer's forum at SF about a month ago and sent you, David and Hal a notification about it to your users.sourceforge.net emails. A few days ago I wondered why no one had replied, and tried if the SF mail aliases even work - and they didn't, at least in the case of my account. So could you please forward this message to the others?

Best regards,
sirius-m

Email #24

Date: Tue, 21 Jul 2009 04:14:43 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

I know this sounds really retarded, but I still haven't been able to get the sourceforge login page to load, so I haven't been able to read it either. https://sourceforge.net/account/login.php

Hal isn't currently actively involved. He helped me a lot defending the design on the Cryptography list, and with initial testing when it was first released. He carried this torch years ago with his Reusable Proof Of Work (RPOW).

I'm not going to be much help right now either, pretty busy with work, and need a break from it after 18 months development.

It would help if there was something for people to use it for. We need an application to bootstrap it. Any ideas?

There are donors I can tap if we come up with something that needs funding, but they want to be anonymous, which makes it hard to actually do anything with it.

mmalmi@cc.hut.fi wrote:
> Hi,
>
> I made a post on the Bitcoin developer's forum at SF about a month ago
> and sent you, David and Hal a notification about it to your
> users.sourceforge.net emails. A few days ago I wondered why no one had
> replied, and tried if the SF mail aliases even work - and they didn't,
> at least in the case of my account. So could you please forward this
> message to the others?
>
> Best regards,
> sirius-m
>

Email #25

Date: Wed, 22 Jul 2009 13:10:02 +0300
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoin

> I know this sounds really retarded, but I still haven't been able to
> get the sourceforge login page to load, so I haven't been able to read
> it either. https://sourceforge.net/account/login.php

That's strange, I haven't had any problems with that. Clearly the banking establishment got scared and banned your account (and founded www.bitcoin.com in attempt to fetch the trademark), eh. You could ask if the SF staff at sfnet_ops@corp.sourceforge.com can help you.

> I'm not going to be much help right now either, pretty busy with work,
> and need a break from it after 18 months development.

Oh, that sounds tough. Take your time.

> It would help if there was something for people to use it for. We need
> an application to bootstrap it. Any ideas?

I've been thinking about a currency exchange service that sells and buys bitcoins for euros and other currencies. Direct exchangeability to an existing currency would give bitcoin the best possible initial liquidity and thus the best adoptability for new users. Everyone accepts payment in coins that are easily exchangeable for common money, but not everyone accepts payment in coins that are only guaranteed to buy a specific kind of a product.

The instructional formula for stable pricing in euros would be something like:

(The amount of euros that you're ready to trade for bc + the euro-value of goods that other people are selling for bc) / (Total number of bc in circulation - own bc assets).

So if there's a total of 1M bitcoins of which you own 100K, you have 1000 eur and no one else trades with bitcoin yet, you can safely offer the exchange rate of 1 eur / 900 bc, without having to devaluate even if everyone sold their coins to you. This could be guaranteed as the minimal exchange rate, but the rate could be also higher when demand is high.

Initially, when others aren't yet offering anything for bitcoins, you can increase your bitcoin assets cheaply - for the minimum price that people bother to do the transaction for. If you had all the existing coins for yourself, you could set the price to whatever you want, because you wouldn't face the risk of having to buy even a single coin with that price (not counting the new money created by others). So it's best to get as much coins as possible before backing bitcoin with all your available euros.

Profit can be gained, as usually in trading, by having a margin between the buying and selling prices. Making Bitcoin as usable as possible will make the business run better, as people do not only want to sell all their coins to you, but also want to buy them and use them as a medium of exchange.

At its simplest this exchange service could be a website where traders, who can be individual persons, can post their rates, and random users can leave trade requests. Some kind of an average rate estimate could be shown on the site. Small-scale trading by individuals would be outside legal hassle in most countries, and putting all the eggs in the same basket would be avoided.

Another idea, which could be additional to the previous one, would be an automated exchange service. The service would automatically calculate the exchange rate and perform the transactions. This would be nicer to the user: completion of the transaction request would be certain and instantaneous. Making this service might actually be quite easy if there was a command line interface to Bitcoin: just take any web application framework and use PayPal back-end integration to automatically send euros when Bitcoins are received, and vice versa. This kind of business would also work great on larger scale if you set up a company and take care of all the bureaucracy needed to practice currency exchange. (I actually have a registered company that I've used for billing of some IT work, I could use that as a base.)

This exchange business thing is something that I'd be interested in doing, and I also have the sufficient technical skills to do it. Although, before this can be done, there should be a non-alpha version of Bitcoin (and the command line interface / API).

> There are donors I can tap if we come up with something that needs
> funding, but they want to be anonymous, which makes it hard to actually
> do anything with it.

If this gets started, donors / high-risk investors would be very welcome to bring capital for the currency's backup.

So, what do you think about the idea? Note that this is not something that I'm asking you to do (unless you want to) if you're busy with other things. I can do it myself, if I get positive reviews about the plan.

Email #26

Date: Wed, 29 Jul 2009 18:14:51 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

I've had quite a few errors coming up when trying to build the third-party libraries and adding them to the Bitcoin build. Do you happen to have a ready-to-build package that you could upload to the CVS or somewhere else? I use mingw + msys, but I guess I could try

Visual C++ also, if it's easier that way.

Email #27

Date: Mon, 24 Aug 2009 06:38:13 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

I got it compile with MinGW + MSYS when I used wxPack instead of just wxWidgets. Maybe wxAdditions was required. The bitcoin.exe filesize was 52MB though, I should see how that can be fixed.

Next I'm going to implement the "minimize to tray" feature and the option to autostart Bitcoin with Windows, so the number of nodes online would stay higher. After that I could see if I can do a Linux port or the command line interface needed for web app frameworks.

Drop by at #bitcoin-dev on FreeNode some time if you use IRC.

And again, thanks for the great work you've done with Bitcoin.

Quote mmalmi@cc.hut.fi:

> I've had quite a few errors coming up when trying to build the
> third-party libraries and adding them to the Bitcoin build. Do you
> happen to have a ready-to-build package that you could upload to the
> CVS or somewhere else? I use mingw + msys, but I guess I could try
> Visual C++ also, if it's easier that way.

Email #28

Date: Mon, 24 Aug 2009 23:00:35 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

That's a good point that since you know how many coins exist and how fast new ones are created, you could set a support price based on the amount of legacy currency you have and be sure you'll have enough to meet all demands. I had imagined an auction, but it would be far simpler and more confidence inspiring to back it at a specific exchange rate.

Offering currency to back bitcoins would attract freebie seekers, with the benefit of attracting a lot of publicity. At first it would mostly be seen as a way to get free money for your computer's idle time. Maybe pitched like help support the future of e-commerce and get a little money for your computer's spare cycles. As people cash in and actually get paid, word would spread exponentially.

It might help to keep the minimum transaction size above an amount which a typical user would be able to accumulate with one computer, so that users have to trade with each other for someone to collect enough to cash in. Aggregators would set up shop to buy bitcoins in smaller increments, which would add confidence in users ability to sell bitcoins if there are more available buyers than just you.

People would obviously be sceptical at first that the backing will hold up against an onslaught of people trying to get the free money, but as the competition raises the proof-of-work difficulty, it should become clear that bitcoins stay scarce. People will see that they can't just get all the bitcoins they want. It would establish a minimum value under bitcoins enabling them to be used for other purposes if, hopefully, other purposes are waiting for something to use.

>> It would help if there was something for people to use it for. We need
>> an application to bootstrap it. Any ideas?
>
> I've been thinking about a currency exchange service that sells and
> buys bitcoins for euros and other currencies. Direct exchangeability
> to an existing currency would give bitcoin the best possible initial
> liquidity and thus the best adoptability for new users. Everyone
> accepts payment in coins that are easily exchangeable for common
> money, but not everyone accepts payment in coins that are only
> guaranteed to buy a specific kind of a product.

That would be more powerful if there was also some narrow product market to use it for. Some virtual currencies like Tencent's Q coin have made headway with virtual goods. It would be sweet if there was some way to

horn in on a market like that as the official virtual currency gets clamped down on with limitations. Not saying it can't work without something, but a ready specific transaction need that it fills would increase the certainty of success.

> At its simplest this exchange service could be a website where
> traders, who can be individual persons, can post their rates, and
> random users can leave trade requests. Some kind of an average rate
> estimate could be shown on the site. Small-scale trading by
> individuals would be outside legal hassle in most countries, and
> putting all the eggs in the same basket would be avoided.

Basically like an eBay site with user reviews to try to establish which sellers can be trusted. The escrow feature will help but not solve everything. It would be far more work to set up such a site than just to set up a single exchange site of your own, and there won't be enough users to make it go until later. I'm thinking it wouldn't make sense to make an eBay type site until later.

> Another idea, which could be additional to the previous one, would be
> an automated exchange service. The service would automatically
> calculate the exchange rate and perform the transactions. This would
> be nicer to the user: completion of the transaction request would be
> certain and instantaneous. Making this service might actually be quite
> easy if there was a command line interface to Bitcoin: just take any
> web application framework and use PayPal back-end integration to
> automatically send euros when Bitcoins are received, and vice versa.
> This kind of business would also work great on larger scale if you set
> up a company and take care of all the bureaucracy needed to practice
> currency exchange. (I actually have a registered company that I've
> used for billing of some IT work, I could use that as a base.)

Even if you had automation, you'd probably want to review orders manually before processing them anyway. It wouldn't be hard to process orders by hand, especially at first. You could always set a minimum order size to keep orders more infrequent.

> This exchange business thing is something that I'd be interested in
> doing, and I also have the sufficient technical skills to do it.
> Although, before this can be done, there should be a non-alpha version
> of Bitcoin (and the command line interface / API).
>
> If this gets started, donors / high-risk investors would be very

> welcome to bring capital for the currency's backup.
>
> So, what do you think about the idea? Note that this is not something
> that I'm asking you to do (unless you want to) if you're busy with
> other things. I can do it myself, if I get positive reviews about the
> plan.

That's great, I could probably get a donor to send currency to you which you convert to euros and pay out through methods that are convenient for users. I don't want to do an exchange business myself, but it can be done independently of me. Like you say, there is more software development to be done first, and also I'd like to keep trying for a while to think of a bootstrap application to use bitcoins for. I've had some ideas that could only be done before an exchange exists.

BTW, I tried to buy bitcoin.com before I started but there was no chance, it's owned by a professional domain speculator. It's normal for open source projects to have .org so it's not so bad.

Email #29

Date: Mon, 24 Aug 2009 23:04:25 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

Glad that worked, it's a pain that the dependencies are so big and hard to build. Some of them give little attention to the Windows build. Next time I update to the latest versions, maybe I'll lay everything out in one directory tree and bundle the whole thing up into a giant archive.

I'm not sure they had wxPack before. I'm glad they got that so everyone doesn't have to build wxWidgets themselves. OpenSSL is the harder one to build.

I reduced the EXE size by running strip.exe on it to take out the debug symbols. That's with mingw. That's the better compiler, I only used VC for debugging.

mmalmi@cc.hut.fi wrote:
> I got it compile with MinGW + MSYS when I used wxPack instead of just
> wxWidgets. Maybe wxAdditions was required. The bitcoin.exe filesize was

> 52MB though, I should see how that can be fixed.
>
> Next I'm going to implement the "minimize to tray" feature and the
> option to autostart Bitcoin with Windows, so the number of nodes online
> would stay higher. After that I could see if I can do a Linux port or
> the command line interface needed for web app frameworks.
>
> Drop by at #bitcoin-dev on FreeNode some time if you use IRC.
>
> And again, thanks for the great work you've done with Bitcoin.
>
> Quote mmalmi@cc.hut.fi:
>
>> I've had quite a few errors coming up when trying to build the
>> third-party libraries and adding them to the Bitcoin build. Do you
>> happen to have a ready-to-build package that you could upload to the
>> CVS or somewhere else? I use mingw + msys, but I guess I could try
>> Visual C++ also, if it's easier that way.
>
>
>

Email #30

Date: Fri, 28 Aug 2009 07:10:06 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

> It might help to keep the minimum transaction size above an amount
> which a typical user would be able to accumulate with one computer, so
> that users have to trade with each other for someone to collect enough
> to cash in. Aggregators would set up shop to buy bitcoins in smaller
> increments, which would add confidence in users ability to sell
> bitcoins if there are more available buyers than just you.

That might be a good idea.

> That would be more powerful if there was also some narrow product
> market to use it for. Some virtual currencies like Tencent's Q coin
> have made headway with virtual goods. It would be sweet if there was
> some way to horn in on a market like that as the official virtual

> currency gets clamped down on with limitations. Not saying it can't
> work without something, but a ready specific transaction need that it
> fills would increase the certainty of success.

Bitcoin could be promoted to the users of virtual communities like World of Warcraft and Second Life, which both have millions of users. It would be great if not only peer-to-peer item traders, but also providers of some existing virtual services that already have a lot of customers, were to adopt the currency early on.

A programming question: What do you think about using the Boost's program_options to write settings like the transaction fee into a file bitcoin.config? Or is it better to save them in the database as it is now? Having a config file would make it easier to change the settings when running the program on a remote server with a console access only.

Email #31

Date: Sat, 29 Aug 2009 18:31:05 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

> Next I'm going to implement the "minimize to tray" feature and the
> option to autostart Bitcoin with Windows, so the number of nodes online
> would stay higher.

Now that I think about it, you've put your finger on the most important missing feature right now that would make an order of magnitude difference in the number of nodes. Without auto-run, we'll almost never retain nodes after an initial tryout interest. Auto-running as a minimized tray icon by default was the key to success for the early file sharing networks. It wouldn't have been appropriate for v0.1.0 when stability wasn't a given yet, but now it's good and stable. This is a must-have feature for the next release so any users that come back to try the new version we hopefully retain this time.

I think the most user friendly way of doing auto-run is putting an icon in the Startup folder. I see OpenOffice.org and a number of other things on my computer do it that way. The other way, creating a runas registry entry, is not easily visible or editable by users, I've never liked that much. I guess what we want is an auto-run option that's on

by default, if the option is changed then it creates or deletes the startup icon.

While it's tempting to do a Linux port, once we do it we have that extra work with every release from then on. I'd rather put it off a while longer. Auto-run might give us 300% more nodes while Linux might give us 3% more. Linux would help server farms, but actually we'd like to favour individual users. Someone reported that it works fine in WinE.

Email #32

Date: Wed, 16 Sep 2009 15:54:42 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Just for information: I committed my working copy to the svn/branches. There's the minimize to tray feature and some other changes. It's nicer to run in the background now, but it's still incomplete and I'm working on it. The bugs are listed in bugs.txt.

Did you get your Sourceforge account work yet?

Email #33

Date: Wed, 30 Sep 2009 19:12:29 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

That's great, that's a good step forward.

Yes, I worked out the sourceforge login problem, it was some tricky thing on the login page that exposed a quirky bug in a browser add-in.

mmalmi@cc.hut.fi wrote:
> Just for information: I committed my working copy to the svn/branches.
> There's the minimize to tray feature and some other changes. It's nicer
> to run in the background now, but it's still incomplete and I'm working
> on it. The bugs are listed in bugs.txt.
>

> Did you get your Sourceforge account work yet?
>

Email #34

Date: Thu, 08 Oct 2009 20:44:49 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

I made a Windows installer for the latest version of Bitcoin, which includes the autostart and minimize to tray features. The installer makes a start menu shortcut and a startup registry entry. I first implemented the autostart with a shortcut to the startup folder, but I found out that it doesn't always work by default and ended up doing it with a registry entry. The registry entry is removed by the uninstaller and can be also disabled from the options menu, so I don't think it's such a big menace to the user after all.

I made the installer with NSIS, and the nsi script can be found in the SVN.

Could you add the installer to the SF download page? Here's the file: http://bitcoin.sourceforge.net/uploads/Bitcoin_setup.exe

There are some new users registered to the bitcoin.sf.net site. One of them just announced that he's trading Bitcoins for dollars. Here's his site: http://newlibertystandard.wetpaint.com/. Making an exchange service first seemed a bit premature for the time being, but on the other hand it's good that people show interest towards the project, and this might attract even more interested people (and hopefully more developers). I just sent the guy an email.

Email #35

Date: Fri, 16 Oct 2009 19:41:40 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Setup, Autorun, v0.1.6

To: mmalmi@cc.hut.fi

Thanks for that. I'm still merging in some changes I had that need to go in before any next release. Some things based on questions and feedback I've received that'll reduce confusion. I'll probably enable multi-proc generating support, and hopefully make it safe to just backup wallet.dat to backup your money. It's good to be coding again!

I'm going to hide the transaction fee setting, which is completely not needed and only serves to confuse people. It was only there for testing and demonstration of a technical detail that can only be needed in the far away future, if ever, but was necessary to implement at the beginning to make it possible later.

What was the problem with the shortcut in the startup folder? If you could send me the code, I'd like to take another look and see if I can see what the problem was. The first strcat in the registry code should be strcpy, otherwise it would fail intermittently. If the same code was in the shortcut one, maybe that was the problem.

It's encouraging to see more people taking an interest such as that NewLibertyStandard site. I like his approach to estimating the value based on electricity. It's educational to see what explanations people adopt. They may help discover a simplified way of understanding it that makes it more accessible to the masses. Many complex concepts in the world have a simplistic explanation that satisfies 80% of people, and a complete explanation that satisfies the other 20% who see the flaws in the simplistic explanation.

mmalmi@cc.hut.fi wrote:
> I made a Windows installer for the latest version of Bitcoin, which
> includes the autostart and minimize to tray features. The installer
> makes a start menu shortcut and a startup registry entry. I first
> implemented the autostart with a shortcut to the startup folder, but I
> found out that it doesn't always work by default and ended up doing it
> with a registry entry. The registry entry is removed by the uninstaller
> and can be also disabled from the options menu, so I don't think it's
> such a big menace to the user after all.
>
> I made the installer with NSIS, and the nsi script can be found in the SVN.
>
> Could you add the installer to the SF download page? Here's the file:
> http://bitcoin.sourceforge.net/uploads/Bitcoin_setup.exe
>
> There are some new users registered to the bitcoin.sf.net site. One of

> them just announced that he's trading Bitcoins for dollars. Here's his
> site: http://newlibertystandard.wetpaint.com/. Making an exchange
> service first seemed a bit premature for the time being, but on the
> other hand it's good that people show interest towards the project, and
> this might attract even more interested people (and hopefully more
> developers). I just sent the guy an email.
>

Email #36

Date: Sun, 18 Oct 2009 18:59:42 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Setup, Autorun, v0.1.6

To: Martti Malmi <mmalmi@cc.hut.fi>

I got it, I see you checked in the startup folder code before changing
it to registry. I don't see any visible problems in the code. I guess
it depends what exactly the problem was with it not always working by
default. Was there a Vista/UAC security problem?

Satoshi Nakamoto wrote:
> What was the problem with the shortcut in the startup folder? If you
> could send me the code, I'd like to take another look and see if I can
> see what the problem was. The first strcat in the registry code should
> be strcpy, otherwise it would fail intermittently. If the same code was
> in the shortcut one, maybe that was the problem.
>
> mmalmi@cc.hut.fi wrote:
>> I made a Windows installer for the latest version of Bitcoin, which
>> includes the autostart and minimize to tray features. The installer
>> makes a start menu shortcut and a startup registry entry. I first
>> implemented the autostart with a shortcut to the startup folder, but I
>> found out that it doesn't always work by default and ended up doing it
>> with a registry entry. The registry entry is removed by the
>> uninstaller and can be also disabled from the options menu, so I don't
>> think it's such a big menace to the user after all.

Email #37

Date: Mon, 19 Oct 2009 00:02:28 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Setup, Autorun, v0.1.6

Well, the code worked and made a shortcut in the startup folder. For some reason it didn't automatically start when booting, but worked fine when you clicked on it in the menu. Now I tried making a shortcut manually, and this time it works on autostart, don't know why. I could try again with the older code.

> I got it, I see you checked in the startup folder code before changing
> it to registry. I don't see any visible problems in the code. I guess
> it depends what exactly the problem was with it not always working by
> default. Was there a Vista/UAC security problem?
>
> Satoshi Nakamoto wrote:
>> What was the problem with the shortcut in the startup folder? If
>> you could send me the code, I'd like to take another look and see
>> if I can see what the problem was. The first strcat in the
>> registry code should be strcpy, otherwise it would fail
>> intermittently. If the same code was in the shortcut one, maybe
>> that was the problem.
>>
>> mmalmi@cc.hut.fi wrote:
>>> I made a Windows installer for the latest version of Bitcoin,
>>> which includes the autostart and minimize to tray features. The
>>> installer makes a start menu shortcut and a startup registry
>>> entry. I first implemented the autostart with a shortcut to the
>>> startup folder, but I found out that it doesn't always work by
>>> default and ended up doing it with a registry entry. The registry
>>> entry is removed by the uninstaller and can be also disabled from
>>> the options menu, so I don't think it's such a big menace to the
>>> user after all.

Email #38

Date: Mon, 19 Oct 2009 00:11:50 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Setup, Autorun, v0.1.6

To: mmalmi@cc.hut.fi

It's possible Bitcoin ran and bailed out because something was wrong. debug.log should tell something if that was the case. What OS are you using? I wonder if we need Admin privilege and don't realize it. Stuff that requires Admin can't start on startup on Vista.

Program shortcuts have multiple tabs of settings with lots of little details. I'll try the startup folder code and see if I can reproduce the problem. Every other systray icon on my computer is in the startup folder, and it makes it easy for users to manage all their autoruns in one place. The things in the registry key tend to be devious hidden bloatware.

I implemented the code to flush wallet.dat whenever it's closed so we'll be able to tell users they only need to backup wallet.dat. You can restore just wallet.dat and it'll re-download the rest. I'll have to do another stress test before release.

mmalmi@cc.hut.fi wrote:
> Well, the code worked and made a shortcut in the startup folder. For
> some reason it didn't automatically start when booting, but worked fine
> when you clicked on it in the menu. Now I tried making a shortcut
> manually, and this time it works on autostart, don't know why. I could
> try again with the older code.
>
>> I got it, I see you checked in the startup folder code before changing
>> it to registry. I don't see any visible problems in the code. I guess
>> it depends what exactly the problem was with it not always working by
>> default. Was there a Vista/UAC security problem?
>>
>> Satoshi Nakamoto wrote:
>>> What was the problem with the shortcut in the startup folder? If
>>> you could send me the code, I'd like to take another look and see
>>> if I can see what the problem was. The first strcat in the
>>> registry code should be strcpy, otherwise it would fail
>>> intermittently. If the same code was in the shortcut one, maybe
>>> that was the problem.
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> I made a Windows installer for the latest version of Bitcoin,
>>>> which includes the autostart and minimize to tray features. The

>>>> installer makes a start menu shortcut and a startup registry
>>>> entry. I first implemented the autostart with a shortcut to the
>>>> startup folder, but I found out that it doesn't always work by
>>>> default and ended up doing it with a registry entry. The registry
>>>> entry is removed by the uninstaller and can be also disabled from
>>>> the options menu, so I don't think it's such a big menace to the
>>>> user after all.
>
>
>
>

Email #39

Date: Tue, 20 Oct 2009 21:38:56 +0300
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Setup, Autorun, v0.1.6

> It's possible Bitcoin ran and bailed out because something was wrong.
> debug.log should tell something if that was the case. What OS are you
> using? I wonder if we need Admin privilege and don't realize it.
> Stuff that requires Admin can't start on startup on Vista.

I'm using XP. I recompiled the older revision and this time the
startup shortcut works. It also works when testing on Vista
(non-admin). Maybe I just missed something the previous time.

> Program shortcuts have multiple tabs of settings with lots of little
> details. I'll try the startup folder code and see if I can reproduce
> the problem. Every other systray icon on my computer is in the startup
> folder, and it makes it easy for users to manage all their autoruns in
> one place. The things in the registry key tend to be devious hidden
> bloatware.

Here it's the other way around, I have all my startup programs in the
registry. But maybe the shortcut method is nicer for the user, if it
works just as well

Email #40

Date: Wed, 21 Oct 2009 18:58:49 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Setup, Autorun, v0.1.6

To: mmalmi@cc.hut.fi

Yeah, I put back your startup folder shortcut code and it started fine for me too on XP and Vista. For good measure, I changed it to make the shortcut settings look identical to one I manually created. I set the working directory to where the EXE is since that's where debug.log is created, otherwise windows puts it in some weird directory. I didn't change the setup script yet.

I checked everything in to SVN (thanks for setting that up)
- multi-proc generate
- flush wallet.dat after every change so the DB doesn't leave that stuff in the transaction logs
- view menu checkbox to hide all generated coins so you can see just your payment transactions
- disabled transaction fee option
- made the minimize to tray options similar to Firefox's MinimizeToTray
- bunch of other misc changes since the 0.1.5 release

I made it not show non-accepted generated coins. It won't show generated coins until they have at least one confirmation (one block linked after it), so usually they'll just never be seen. Occasionally a generated coin that was displayed might disappear because it became not accepted later. I don't think anyone would notice the occasional non-accepteds if we didn't point them out in the UI. People have told me they find it annoying to have to look at them, as they're permanently displayed in the transaction record.

I still have more testing to do. I guess we gotta test Windows 7 now.

mmalmi@cc.hut.fi wrote:
>> It's possible Bitcoin ran and bailed out because something was wrong.
>> debug.log should tell something if that was the case. What OS are you
>> using? I wonder if we need Admin privilege and don't realize it.
>> Stuff that requires Admin can't start on startup on Vista.
>
> I'm using XP. I recompiled the older revision and this time the startup
> shortcut works. It also works when testing on Vista (non-admin). Maybe I

> just missed something the previous time.
>
>> Program shortcuts have multiple tabs of settings with lots of little
>> details. I'll try the startup folder code and see if I can reproduce
>> the problem. Every other systray icon on my computer is in the startup
>> folder, and it makes it easy for users to manage all their autoruns in
>> one place. The things in the registry key tend to be devious hidden
>> bloatware.
>
> Here it's the other way around, I have all my startup programs in the
> registry. But maybe the shortcut method is nicer for the user, if it
> works just as well
>

Email #41

Date: Sat, 24 Oct 2009 00:55:06 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: [bitcoin-list] Does Bitcoin Crash in Windows?

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: bitcoin-list@lists.sourceforge.net

Liberty Standard wrote:
> Do you Windows users experience occasional Bitcoin crashes?
> Lately Bitcoin running in wine-1.0.1 has been crashing frequently. I was
> just wondering whether this is a Wine issue or a Bitcoin issue.

I haven't had any reports of crashes in v0.1.5. It's been rock solid
for me on Windows. I think it must be Wine related. If you get another
crash in Wine and it prints anything on the terminal, e-mail me and I
may be able to figure out what happened, maybe something I can work
around. Martti and I have been working on a new version to release soon
and it would be nice to get any Wine fixes in there.

> The following four lines print from the terminal when I start Bitcoin.
> fixme:toolhelp:CreateToolhelp32Snapshot Unimplemented: heap list snapshot
> fixme:toolhelp:Heap32ListFirst : stub
> fixme:toolhelp:CreateToolhelp32Snapshot Unimplemented: heap list snapshot
> fixme:toolhelp:Heap32ListFirst : stub

Those don't look like anything to worry about. Probably functions
unimplemented by Wine that are harmlessly stubbed out.

> I previously wasn't starting Bitcoin from the terminal, so I don't know what
> gets printed out when it crashes, but I'll reply with the results the next
> time it crashes.
>
> While Bitcoin first downloads previously completed blocks, the file
> debug.log grows grows to 17.4 MB and then stops growing. I imagine it will
> continue to grow as more bitcoins are completed.

You can delete debug.log occasionally if you don't want to take the disk
space. It's just status messages that help with debugging.

bitcoin.sourceforge.net looks fine now. Maybe sourceforge was doing
some maintenance.

Satoshi

Email #42

Date: Mon, 26 Oct 2009 17:50:10 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Fw: bitcoin.sourceforge.net
To: Martti Malmi <mmalmi@cc.hut.fi>

Any idea what's going on with it? Every time I look, it's fine.

Eugen Leitl wrote:
On Sat, Oct 24, 2009 at 12:55:06AM +0100, Satoshi Nakamoto wrote:
 > > bitcoin.sourceforge.net looks fine now. Maybe sourceforge was doing

Doesn't work right now.

> > some maintenance.

Liberty Standard wrote:
> In case you weren't aware, the Bitcoin website is down.
>
> http://bitcoin.sourceforge.net/
>
> -----
> You are running bitweaver in TEST mode
>
> * Click here to log a bug, if this appears to be an error with the
> application.
> * Go here to begin the installation process, if you haven't done so
> already.
> * To hide this message, please set the IS_LIVE constant to TRUE
in your
> kernel/config_inc.php file.

Email #43

Date: Tue, 27 Oct 2009 05:02:49 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fw: bitcoin.sourceforge.net

IS_LIVE option was indeed set to false, but it only affects the
visibility of error messages to user. I've noticed the site being slow
at times, sometimes taking up to 30 seconds to load. I think it's
related to the Sourceforge hosting. Bitweaver should be among the
lightest PHP CMS'es, but I can check out if there are any issues to it.

Off the topic, do you think that we could use Boost's thread and
socket libraries instead of the Windows-specific ones? Are there other
windows-only-functions used in the code?

> Any idea what's going on with it? Every time I look, it's fine.
>
>
> Eugen Leitl wrote:
> On Sat, Oct 24, 2009 at 12:55:06AM +0100, Satoshi Nakamoto wrote:
>> > bitcoin.sourceforge.net looks fine now. Maybe sourceforge was doing

>
> Doesn't work right now.
>
>> > some maintenance.
>
>
> Liberty Standard wrote:
>> In case you weren't aware, the Bitcoin website is down.
>>
>> http://bitcoin.sourceforge.net/
>>
>> -----
>> You are running bitweaver in TEST mode
>>
>>   * Click here to log a bug, if this appears to be an error with the
>> application.
>>   * Go here to begin the installation process, if you haven't done so
>> already.
>>   * To hide this message, please set the IS_LIVE constant to TRUE in your
>> kernel/config_inc.php file.

Email #44

Date: Tue, 27 Oct 2009 04:45:47 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fw: bitcoin.sourceforge.net

To: mmalmi@cc.hut.fi

Sourceforge is just so darn slow. I don't know what else to do though.
  It's such a standard, more often than not any given project has a
projectname.sourceforge.net site. When I see whatever.sourceforge.net
in a google search, I assume that's the official site.

Is there a way to make Bitweaver allow users to edit (and maybe delete)
their own messages in the forum?

Getting antsy to port to Linux? It's not a decision to be taken lightly
because once it's done, it doubles my testing and building workload.
Although I am worried about Liberty's Wine crashes.

I've tried to be as portable as possible and use standard C stuff instead of Windows calls. The threading is _beginthread which is part of the standard C library. wxWidgets has wxCriticalSection stuff we can use. The sockets code is send/recv stuff which I think is the same as unix because Microsoft ported sockets from BSD. We need direct control over sockets, it wouldn't be a good idea to get behind an abstraction layer. wxWidgets is a good place to look for cross-platform support functions. I want to avoid #ifdefing up the code if we can. Anything that's used more than once probably becomes a function in util.cpp that has the #ifdef in it.

BTW, I have a lot of uncommitted changes right now because it includes some crucial protocol transitions that can't be unleashed on the network until I've tested the heck out of it. It shouldn't be too much longer.

Can you make the setup uninstall the Startup folder icon? I figure it should install and uninstall an icon in a regular program group, and just uninstall the Startup folder one. I guess it doesn't matter that much whether it installs and uninstalls the Startup folder icon or just uninstalls it.

mmalmi@cc.hut.fi wrote:
> IS_LIVE option was indeed set to false, but it only affects the
> visibility of error messages to user. I've noticed the site being slow
> at times, sometimes taking up to 30 seconds to load. I think it's
> related to the Sourceforge hosting. Bitweaver should be among the
> lightest PHP CMS'es, but I can check out if there are any issues to it.
>
> Off the topic, do you think that we could use Boost's thread and socket
> libraries instead of the Windows-specific ones? Are there other
> windows-only-functions used in the code?
>
>> Any idea what's going on with it? Every time I look, it's fine.
>>
>>
>> Eugen Leitl wrote:
>> On Sat, Oct 24, 2009 at 12:55:06AM +0100, Satoshi Nakamoto wrote:
>>> > bitcoin.sourceforge.net looks fine now. Maybe sourceforge was doing
>>
>> Doesn't work right now.
>>
>>> > some maintenance.
>>

>>
>> Liberty Standard wrote:
>>> In case you weren't aware, the Bitcoin website is down.
>>>
>>> http://bitcoin.sourceforge.net/
>>>
>>> -----
>>> You are running bitweaver in TEST mode
>>>
>>> * Click here to log a bug, if this appears to be an error with the
>>> application.
>>> * Go here to begin the installation process, if you haven't done so
>>> already.
>>> * To hide this message, please set the IS_LIVE constant to TRUE
>>> in your
>>> kernel/config_inc.php file.
>
>
>

Email #45

Date: Wed, 28 Oct 2009 23:27:35 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fw: bitcoin.sourceforge.net

> Sourceforge is just so darn slow. I don't know what else to do though.
> It's such a standard, more often than not any given project has a
> projectname.sourceforge.net site. When I see whatever.sourceforge.net
> in a google search, I assume that's the official site.
>
> Is there a way to make Bitweaver allow users to edit (and maybe delete)
> their own messages in the forum?

It's not possible with the current version of Bitweaver. Bitweaver's
wiki and forum packages aren't so very highly advanced. SF hosting
also has its disadvantages, like the occasional slowness and lack of
e-mailer and user IP retrieving. I've been considering to buy web
hosting from prq.se (the host of Wikileaks and Pirate Bay, among
others) to be used later for the exchange service. I could maybe host
the project site there as well, under a separate user account for

better security. There I could set up Drupal or TikiWiki, which are more advanced and have quite a lot bigger and more active developer/user communities than Bitweaver.

> Getting antsy to port to Linux? It's not a decision to be taken
> lightly because once it's done, it doubles my testing and building
> workload. Although I am worried about Liberty's Wine crashes.
>
> I've tried to be as portable as possible and use standard C stuff
> instead of Windows calls. The threading is _beginthread which is part
> of the standard C library. wxWidgets has wxCriticalSection stuff we
> can use. The sockets code is send/recv stuff which I think is the same
> as unix because Microsoft ported sockets from BSD. We need direct
> control over sockets, it wouldn't be a good idea to get behind an
> abstraction layer. wxWidgets is a good place to look for
> cross-platform support functions. I want to avoid #ifdefing up the
> code if we can. Anything that's used more than once probably becomes a
> function in util.cpp that has the #ifdef in it.

Ok. I replaced the Windows thread and socket library includes with their POSIX equivalents, and now it only gives a few errors, mostly svn/branches, it doesn't need to be an official release yet.

> Can you make the setup uninstall the Startup folder icon? I figure it
> should install and uninstall an icon in a regular program group, and
> just uninstall the Startup folder one. I guess it doesn't matter that
> much whether it installs and uninstalls the Startup folder icon or just
> uninstalls it.

I'll do it.

Email #46

Date: Thu, 29 Oct 2009 02:05:30 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fw: bitcoin.sourceforge.net

To: mmalmi@cc.hut.fi

I'll convert the CriticalSection code to wxCriticalSection and upload it to SVN (it's a little tricky). I don't know what to do for TryEnterCriticalSection though. I think I'm almost ready to check everything in.

You're probably right, it's about time to do a linux build. I've been working on getting my linux machine set up and building the dependencies.

> Ok. I replaced the Windows thread and socket library includes with their
> POSIX equivalents, and now it only gives a few errors, mostly from the
> CriticalSections. If I make it work, I'll put it into svn/branches, it
> doesn't need to be an official release yet.

Email #47

Date: Thu, 29 Oct 2009 06:08:10 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fw: bitcoin.sourceforge.net

> I'll convert the CriticalSection code to wxCriticalSection and upload
> it to SVN (it's a little tricky). I don't know what to do for
> TryEnterCriticalSection though. I think I'm almost ready to check
> everything in.

Would the Boost mutex be of any help here?

http://www.boost.org/doc/libs/1_40_0/doc/html/thread/synchronization.html#thread.synchronization.mutex_concepts

Email #48

Date: Thu, 29 Oct 2009 06:38:30 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: mmalmi@cc.hut.fi

The easy solution I took was to look at the wxWidgets source code and see how they did it. They just mapped it to wxMutex on non-MSW, which does have TryEnter, so that mapped in perfectly.

I checked in all my backlog of changes to SVN, including the overhaul of CCriticalSection in util.h and OpenSSL's mutex callback in util.cpp to

do everything with wxWidgets when not on Windows.

If we get it working on Linux, I'll run my test suite against it here
off-network first, then we can give an unreleased build to
LibertyStandard to test for a while before going public.

mmalmi@cc.hut.fi wrote:
>> I'll convert the CriticalSection code to wxCriticalSection and upload
>> it to SVN (it's a little tricky). I don't know what to do for
>> TryEnterCriticalSection though. I think I'm almost ready to check
>> everything in.
>
> Would the Boost mutex be of any help here?
>
>
http://www.boost.org/doc/libs/1_40_0/doc/html/thread/synchronization.html#thread.synchroniz
ation.mutex_concepts
>
>

Email #49

Date: Fri, 30 Oct 2009 01:05:45 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: Martti Malmi <mmalmi@cc.hut.fi>

I fixed some non-portable stuff I came across:
QueryPerformanceCounter
%I64d in printf format strings
Sleep
CheckDiskSpace

If there's any other unportable stuff you know of I should fix, let me know.

I think I'll move debug.log and db.log into the same directory as the
data files (%appdata%\Bitcoin), rather than whatever the current
directory happens to be.

Email #50

Date: Sat, 31 Oct 2009 11:21:50 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

I made an #ifdef to replace QueryPerformanceCounter with Linux's
gettimeofday in util.h. Some Unicode/ANSI errors were resolved without
code changes when I updated to wxWidgets 2.9. The only compile error
I'm getting in Linux at the moment is from heapchk() in util.h.

> I fixed some non-portable stuff I came across:
> QueryPerformanceCounter
> %I64d in printf format strings
> Sleep
> CheckDiskSpace
>
> If there's any other unportable stuff you know of I should fix, let me know.
>
> I think I'll move debug.log and db.log into the same directory as the
> data files (%appdata%\Bitcoin), rather than whatever the current
> directory happens to be.

Email #51

Date: Sat, 31 Oct 2009 20:09:58 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: mmalmi@cc.hut.fi

heapchk() is just a MSVCRT debugging thing that's not being used. It
can be a no-op on Linux. OpenSSL automatically uses /dev/urandom to
seed on Linux, so RandAddSeedPerfmon can also be a no-op.

Don't let it connect to the network before we've tested it thoroughly
off-net. If you have two computers, unplug the internet and use
"bitcoin -connect=<ip>" to connect to each other, one windows and one
linux. -connect will allow you to connect to non-routable addresses

like 192.168.x.x. We don't want to reflect badly on the reliability of the network if it throws off some malformed crud we hadn't thought to check for yet, or discovers something else anti-social to do on the network.

I have time that I can do some testing when you've got something buildable to test. I can include it in the stress test I'm currently running on the changes so far.

mmalmi@cc.hut.fi wrote:
> I made an #ifdef to replace QueryPerformanceCounter with Linux's
> gettimeofday in util.h. Some Unicode/ANSI errors were resolved without
> code changes when I updated to wxWidgets 2.9. The only compile error I'm
> getting in Linux at the moment is from heapchk() in util.h.
>
>> I fixed some non-portable stuff I came across:
>> QueryPerformanceCounter
>> %I64d in printf format strings
>> Sleep
>> CheckDiskSpace
>>
>> If there's any other unportable stuff you know of I should fix, let me
>> know.
>>
>> I think I'll move debug.log and db.log into the same directory as the
>> data files (%appdata%\Bitcoin), rather than whatever the current
>> directory happens to be.
>
>
>

Email #52

Date: Tue, 03 Nov 2009 09:31:41 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

I uploaded what I've ported so far to the svn/branches. Util, script, db and the headers compile fully now and net.cpp partially, so there's still work to do.

_beginthread doesn't have a direct Linux equivalent, so I used Boost

threads instead.

I couldn't get connected using the Tor SOCKS proxy. That might be
because of the Freenode Tor policy which requires connecting to their
hidden service: http://freenode.net/irc_servers.shtml#tor

> heapchk() is just a MSVCRT debugging thing that's not being used. It
> can be a no-op on Linux. OpenSSL automatically uses /dev/urandom to
> seed on Linux, so RandAddSeedPerfmon can also be a no-op.
>
> Don't let it connect to the network before we've tested it thoroughly
> off-net. If you have two computers, unplug the internet and use
> "bitcoin -connect=<ip>" to connect to each other, one windows and one
> linux. -connect will allow you to connect to non-routable addresses
> like 192.168.x.x. We don't want to reflect badly on the reliability of
> the network if it throws off some malformed crud we hadn't thought to
> check for yet, or discovers something else anti-social to do on the
> network.
>
> I have time that I can do some testing when you've got something
> buildable to test. I can include it in the stress test I'm currently
> running on the changes so far.
>
> mmalmi@cc.hut.fi wrote:
>> I made an #ifdef to replace QueryPerformanceCounter with Linux's
>> gettimeofday in util.h. Some Unicode/ANSI errors were resolved
>> without code changes when I updated to wxWidgets 2.9. The only
>> compile error I'm getting in Linux at the moment is from heapchk()
>> in util.h.
>>
>>> I fixed some non-portable stuff I came across:
>>> QueryPerformanceCounter
>>> %I64d in printf format strings
>>> Sleep
>>> CheckDiskSpace
>>>
>>> If there's any other unportable stuff you know of I should fix,
>>> let me know.
>>>
>>> I think I'll move debug.log and db.log into the same directory as the
>>> data files (%appdata%\Bitcoin), rather than whatever the current
>>> directory happens to be.
>>

>>
>>

Email #53

Date: Tue, 03 Nov 2009 15:53:25 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Linux build, proxy
To: mmalmi@cc.hut.fi

Great, I've been looking forward to working on the Linux build.

If you connect to Freenode's hidden service, then they tell you they've also banned TOR from that due to abuse and it kicks you off. There's a several step procedure you can do to run a password utility on unix and e-mail request an account that you could login with, but that's getting pretty complicated. I wonder if we could get away with applying for one account and then everyone use the same account? I suppose the IRC server probably limits accounts to one login, or some admin might not like to see a dozen logins on the same account.

Besides the IRC part, how did your test of proxy go? Since you've been connected before, your addr.dat contains known node addresses, but without IRC to know which ones are online, it takes a long time to find them. There are normally 1 to 3 other nodes besides you that can accept incoming connections, and existing nodes that already know you would eventually connect to you. How many connections did you get, and how long did it take? I guess to know whether it successfully connected outbound through TOR you'd need to search debug.log for "connected".

To originally connect with TOR without connecting normally once to get seeded, you'd have to know the address of an existing node that can accept incoming connections and seed it like this:
bitcoin -proxy=127.0.0.1:9050 -addnode=<ip of a node>

If some nodes that accept incoming connects were willing to have their IP coded into the program, it could seed automatically. Or some IP seed addresses posted on a Wiki page with the instructions.

Another option is to search the world again for an IRC server that

doesn't ban TOR nodes. Or if we could get someone to set one up. IRC servers ban TOR because they have actual text chat on them... if there was one with just bots and junk then it wouldn't care. Probably should post a question on the forum or the mailing list and see if anyone knows one.

Another problem is that TOR users can't accept incoming connections, and we have so few that can. If everyone goes to TOR, there won't be any nodes to connect to.

We have a shortage of nodes that can accept incoming connections. It generally ranges from 2 to 4 lately. We need to emphasize the importance to people of setting up port forwarding on their router. Every P2P file sharing program has instructions how to do it. We should have a paragraph on the bitcoin.sourceforge.net homepage urging people to set up port forwarding to accept incoming connections, and a link to a site that describes how to do it for each router.

mmalmi@cc.hut.fi wrote:
> I uploaded what I've ported so far to the svn/branches. Util, script, db
> and the headers compile fully now and net.cpp partially, so there's
> still work to do.
>
> _beginthread doesn't have a direct Linux equivalent, so I used Boost
> threads instead.
>
> I couldn't get connected using the Tor SOCKS proxy. That might be
> because of the Freenode Tor policy which requires connecting to their
> hidden service: http://freenode.net/irc_servers.shtml#tor
>
>> heapchk() is just a MSVCRT debugging thing that's not being used. It
>> can be a no-op on Linux. OpenSSL automatically uses /dev/urandom to
>> seed on Linux, so RandAddSeedPerfmon can also be a no-op.
>>
>> Don't let it connect to the network before we've tested it thoroughly
>> off-net. If you have two computers, unplug the internet and use
>> "bitcoin -connect=<ip>" to connect to each other, one windows and one
>> linux. -connect will allow you to connect to non-routable addresses
>> like 192.168.x.x. We don't want to reflect badly on the reliability of
>> the network if it throws off some malformed crud we hadn't thought to
>> check for yet, or discovers something else anti-social to do on the
>> network.
>>

>> I have time that I can do some testing when you've got something
>> buildable to test. I can include it in the stress test I'm currently
>> running on the changes so far.
>>
>> mmalmi@cc.hut.fi wrote:
>>> I made an #ifdef to replace QueryPerformanceCounter with Linux's
>>> gettimeofday in util.h. Some Unicode/ANSI errors were resolved
>>> without code changes when I updated to wxWidgets 2.9. The only
>>> compile error I'm getting in Linux at the moment is from heapchk()
>>> in util.h.
>>>
>>>> I fixed some non-portable stuff I came across:
>>>> QueryPerformanceCounter
>>>> %I64d in printf format strings
>>>> Sleep
>>>> CheckDiskSpace
>>>>
>>>> If there's any other unportable stuff you know of I should fix, let
>>>> me know.
>>>>
>>>> I think I'll move debug.log and db.log into the same directory as the
>>>> data files (%appdata%\Bitcoin), rather than whatever the current
>>>> directory happens to be.
>>>
>>>
>>>
>
>
>

Email #54

Date: Wed, 04 Nov 2009 05:38:17 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: mmalmi@cc.hut.fi

It was almost there. I fixed a few things and got it to finish
compiling but I don't know the system libraries to link to so there's
undefined references galore.

I changed the makefile to look for things under /usr/local and in their

default "make install" locations. I wrote what I did and switches I used in build-unix.txt. I'm currently using wxWidgets 2.8.9 for now because it's the same version as on Windows and I don't want to wonder if there's version change issues at the same time as platform change. 2.8.10 or 2.9.0 are probably fine though. I went with the single-library compile of wxWidgets since we're linking to almost every library anyway.

I added xpm files, which is what they use everywhere else but Windows instead of RC files. They're clever C files that define graphics in static arrays. The bitcoin icon has 5 different versions but I couldn't figure out how that works in xpm so I only put the biggest one. Maybe on GTK it scales it for you. I don't know if these are right or what, but they compile.

mmalmi@cc.hut.fi wrote:
> I uploaded what I've ported so far to the svn/branches. Util, script, db
> and the headers compile fully now and net.cpp partially, so there's
> still work to do.
>
> _beginthread doesn't have a direct Linux equivalent, so I used Boost
> threads instead.
>

Email #55

Date: Wed, 04 Nov 2009 20:38:03 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: mmalmi@cc.hut.fi

Just letting you know I'm still working on the Linux build so we don't duplicate work. I got it linked and ran it and working through runtime issues like getting it switched to load bitmaps from xpm instead of resources.

There are debian packages available for some of the dependencies instead of having to compile them ourselves:
apt-get install build-essential
apt-get install libgtk2.0-dev
apt-get install libssl-dev

I need to see if Berkeley DB or Boost have packages.

We'll shared-link OpenSSL, I'm pretty sure it's always preinstalled on Linux. GTK has to be shared linked. I'm not completely sure if it's preinstalled by default.

Email #56

Date: Wed, 04 Nov 2009 23:42:44 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

> Besides the IRC part, how did your test of proxy go? Since you've been
> connected before, your addr.dat contains known node addresses, but
> without IRC to know which ones are online, it takes a long time to find
> them. There are normally 1 to 3 other nodes besides you that can
> accept incoming connections, and existing nodes that already know you
> would eventually connect to you. How many connections did you get, and
> how long did it take? I guess to know whether it successfully
> connected outbound through TOR you'd need to search debug.log for
> "connected".

Enabling the proxy setting and restarting Bitcoin I got the first connections in less than a minute and ultimately even 8 connections. I wonder if they're all really through TOR. Netstat shows only 2 connections to localhost:9050 and 7 connections from local port 8333 to elsewhere. (Some of the shown connections may be already disconnected ones.) For some reason there's no debug.log in the folder where I'm running it.

> If some nodes that accept incoming connects were willing to have their
> IP coded into the program, it could seed automatically. Or some IP
> seed addresses posted on a Wiki page with the instructions.

The wiki page sounds like a good and quickly applicable solution. I could keep my ip updated there and we could ask others to do the same. When the Linux build works, it's easier to set up nodes on servers that are online most of the time and have a static IP. A static ip list shipped with Bitcoin and a peer exchange protocol would be cool. That way there'd be no need for an IRC server.

> Just letting you know I'm still working on the Linux build so we don't

> duplicate work. I got it linked and ran it and working through runtime
> issues like getting it switched to load bitmaps from xpm instead of
> resources.

Ok. I didn't get it linked on the first attempt, but I didn't look
further into the dependencies yet.

Email #57

Date: Thu, 05 Nov 2009 05:31:03 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Linux build
To: Martti Malmi <mmalmi@cc.hut.fi>

I merged the linux changes into the main trunk on SVN. It compiles and
runs now. I think all the problems are in the UI. The menus quickly
quit working and it doesn't repaint when it's supposed to unless I
resize it, and the UI is getting some segfaults. Shouldn't be too hard
to debug with gdb. I haven't tested if it plays nice with other nodes
yet so keep it off-net.

build-unix.txt and makefile.unix added

Email #58

Date: Thu, 05 Nov 2009 15:25:27 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Proxy
To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> Enabling the proxy setting and restarting Bitcoin I got the first
> connections in less than a minute and ultimately even 8 connections. I
> wonder if they're all really through TOR. Netstat shows only 2
> connections to localhost:9050 and 7 connections from local port 8333 to
> elsewhere. (Some of the shown connections may be already disconnected
> ones.) For some reason there's no debug.log in the folder where I'm
> running it.

debug.log moved to the data directory "%appdata%/bitcoin/debug.log"

7 inbound and 2 outbound sounds about as expected.

My last SVN commit included an overhaul of the code that selects the order of addresses to connect to, trying them in the order of most recently seen online, so it should get connected in a more reasonable amount of time if IRC is unavailable. IRC is really only needed to seed the first connection, but we've been using it as a crutch to get connected faster.

>> If some nodes that accept incoming connects were willing to have their
>> IP coded into the program, it could seed automatically. Or some IP
>> seed addresses posted on a Wiki page with the instructions.
>
> The wiki page sounds like a good and quickly applicable solution. I
> could keep my ip updated there and we could ask others to do the same.
> When the Linux build works, it's easier to set up nodes on servers that
> are online most of the time and have a static IP. A static ip list
> shipped with Bitcoin and a peer exchange protocol would be cool. That
> way there'd be no need for an IRC server.

That would be great. It's only TOR users that need it, so in the instructions saying "bitcoin -proxy=127.0.0.1:9050 -addnode=<someip>", someip could be an actual static IP, with the wiki free-for-all add-your-ip list nearby or a link to it. There should be a link to that optional step, add your IP to this list now that you can accept incoming if you're static.

Do you think anonymous people are looking to be completely stealth, as in never connect once without TOR so nobody knows they use bitcoin, or just want to switch to TOR before doing any transactions? It's just if you want to be completely stealth that you'd have to go through the -proxy -addnode manual seeding. It would be very easy to fumble that up; if you run bitcoin normally to begin with it immediately automatically starts connecting.

Email #59

Date: Thu, 05 Nov 2009 17:33:58 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Forum

To: Martti Malmi <mmalmi@cc.hut.fi>

Now that the forum on bitcoin.sourceforge.net is catching on, we really should look for somewhere that freehosts full blown forum software. The bitweaver forum feature is just too lightweight. I assume the "Forum" tab on the homepage can link out to wherever the forum is hosted.

I've seen projects that have major following just from forum talk and pie-in-the-sky planning without even having any code yet. Having a lot of forum talk gives a project more presence on the net, more search hits, makes it look big, draws new users in, helps solve support questions, hashes out what features are most of wanted.

It would be a big plus if it could support SSL, at least for the login page if not sitewide. Multiple people on the forum have expressed interest in TOR/I2P, and those users need SSL because a lot of TOR exit nodes are probably password scrapers run by identity thieves. A lot of the core interest in Bitcoin is going to be from the privacy crowd.

Any ideas where we can get a free forum? Maybe we should look at where some other projects have their forums hosted for ideas where to look.

Email #60

Date: Fri, 06 Nov 2009 06:20:15 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: Martti Malmi <mmalmi@cc.hut.fi>

It works reliably on Linux now, except if it uses wxMessageBox() outside the GUI thread, it'll crash because non-GUI threads can't open a window on Linux. I haven't got to fixing that yet. I've been running my stress test on it and it's functioning normally.

Most of wxWidgets is not thread-safe to use in threads other than the UI thread, but as a rule of thumb on Windows anything not UI related is OK. It turns out its more thread-unsafe on GTK. I replaced a bunch of stuff at once so I don't know if it was just one thing (probably Repaint), but I have to assume even any wx function that uses wxString is not safe to use outside the UI thread. So dang, there goes all the nice wxWidgets portability support functions. I left a few simple

things like wxThread::GetCPUCount() that I checked the source and it's all numerical, and wxMutex has to be safe or it'd be useless.

There's an issue that if you exit and run it again right away, it can't bind port 8333. The port frees up after about a minute. Unless I'm missing something, I am closing the socket before exit, so I don't know what else I can do. Maybe this is just something about Linux that it takes a minute to free up a port you had bound. Possibly a security feature so some trojan doesn't kill the web server and quickly jump into its place and pick up all the client retries.

Still gotta figure out how to do the xpm version of the icon correctly.

I wonder if the database dat files are interchangeable with Windows.

Email #61

Date: Sat, 07 Nov 2009 12:13:45 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

> Do you think anonymous people are looking to be completely stealth, as
> in never connect once without TOR so nobody knows they use bitcoin, or
> just want to switch to TOR before doing any transactions? It's just if
> you want to be completely stealth that you'd have to go through the
> -proxy -addnode manual seeding. It would be very easy to fumble that
> up; if you run bitcoin normally to begin with it immediately
> automatically starts connecting.

The people who are interested in being stealthy tend to be more technically able, and they probably don't have a problem following the instructions to get perfect secrecy. Of course there could be a connect-button in the UI that needs to be clicked before use, but the tradeoff is that the UI becomes less straightforward for the average user.

> It would be a big plus if it could support SSL, at least for the login
> page if not sitewide. Multiple people on the forum have expressed
> interest in TOR/I2P, and those users need SSL because a lot of TOR exit
> nodes are probably password scrapers run by identity thieves. A lot of
> the core interest in Bitcoin is going to be from the privacy crowd.
>

> Any ideas where we can get a free forum? Maybe we should look at where
> some other projects have their forums hosted for ideas where to look.

One option would be ning.com. Ning.com is a popular community site and many users who already have an account wouldn't need to register a new account. Example: http://p2pfoundation.ning.com/. This seems to support SSL.

Another option would be to relocate the whole site to some place where we can run Drupal or TikiWiki. I've been thinking of buying virtual server or web hosting for the exchange service sometime soon, and if the platform allows for two separate accounts, we could run the site there too. The CMS and its database can be always copied and relocated to a new web host if needed.

Email #62

Date: Sun, 08 Nov 2009 05:23:13 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Linux build ready for testing (attached)

To: Martti Malmi <mmalmi@cc.hut.fi>, Liberty Standard <newlibertystandard@gmail.com>

bitcoin-linux-0.1.6-test1.tar.bz2 attached

Email #63

Date: Sun, 08 Nov 2009 05:52:11 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Linux build ready for testing

To: Martti Malmi <mmalmi@cc.hut.fi>, Liberty Standard <newlibertystandard@gmail.com>

The Linux build is ready for testing on the network. It seems solid. I sent the executable as an attachment in the previous e-mail, but if the mail server didn't let it through (it's 12MB), you can download it here: http://rapidshare.com/files/303914158/linux-0.1.6-test1.tar.bz2.html

Email #64

Date: Sun, 08 Nov 2009 11:50:44 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Cc: Liberty Standard <newlibertystandard@gmail.com>

Subject: Re: Linux build ready for testing

That's great! A major waypoint reached. Seems to work fine here.

> The Linux build is ready for testing on the network. It seems solid.
> I sent the executable as an attachment in the previous e-mail, but if
> the mail server didn't let it through (it's 12MB), you can download it
> here:
> http://rapidshare.com/files/303914158/linux-0.1.6-test1.tar.bz2.html

Email #65

Date: Sun, 08 Nov 2009 18:48:27 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

I made a ning.com site for testing: bitcoin.ning.com. At least it's
there to get Google hits, even if we didn't use it.

> Now that the forum on bitcoin.sourceforge.net is catching on, we really
> should look for somewhere that freehosts full blown forum software.
> The bitweaver forum feature is just too lightweight. I assume the
> "Forum" tab on the homepage can link out to wherever the forum is
> hosted.
>
> I've seen projects that have major following just from forum talk and
> pie-in-the-sky planning without even having any code yet. Having a lot
> of forum talk gives a project more presence on the net, more search
> hits, makes it look big, draws new users in, helps solve support
> questions, hashes out what features are most of wanted.
>
> It would be a big plus if it could support SSL, at least for the login
> page if not sitewide. Multiple people on the forum have expressed
> interest in TOR/I2P, and those users need SSL because a lot of TOR exit

> nodes are probably password scrapers run by identity thieves. A lot of
> the core interest in Bitcoin is going to be from the privacy crowd.
>
> Any ideas where we can get a free forum? Maybe we should look at where
> some other projects have their forums hosted for ideas where to look.

Email #66

Date: Sun, 08 Nov 2009 17:39:39 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build ready for testing

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

In the debug.log, it requests the block list, receives the block list, then begins uploading the list of blocks requested. It doesn't receive the blocks, but it didn't run long enough for me to be sure it would have had time yet. Everything else looks normal.

How long did you run it? It could take a few minutes to start downloading the blocks. Especially if you're on a cable modem, the uplink can be much lower bandwidth so it would take some time to upload the block request list.

If you run it again and it still doesn't download blocks, keep it running for several hours at least and then send me the debug.log. That should give it time for my node to connect to you and I could see what it says on my side and correlate it with your debug.log.

You're right about the minimize on close option, there's no reason that can't be separate. Martti originally had it separate and I made it a sub-option, my bad. I'll change it back.

Liberty Standard wrote:
> That is what I meant. The blocks displayed in the status bar did not
> increase at all while i ran the program. I have attached my debug.log.
>
> A good way for you to test the tray icon in Gnome is to remove the
> notification area and then add it back. If the icon is still displayed
> after adding the notification back, then it's working correctly.

> I generally set application preferences to not minimize to the tray, but
> to close to the tray. And I keep the application minimized. That way I
> don't accidentally close the program and still have the convenience of
> being able to open the application from the tray. (I don't display open
> windows in the 'task bar' but I have an icon that if clicked displays
> open windows as sub-menu items.) Then if the tray icon disappears, I go
> into the settings disable and re-enable the tray icon setting to get it
> to reappear. That's currently not possible with the bitcoin preferences
> because the close to tray check mark can not be enabled without the
> minimize to tray check box being enabled.
>
>
> On Sun, Nov 8, 2009 at 9:08 AM, Satoshi Nakamoto <satoshin@gmx.com
> <mailto:satoshin@gmx.com>> wrote:
>
>   Liberty Standard wrote:
>
>   I downloaded it and it runs. It and it is using plenty of CPU,
>   so I think it's working properly. It has not downloaded
>   previously generated blocks. Is that a bug or a new feature?
>
>
>   If you mean the blocks count in the status bar isn't working its way
>   up to around 26600, then that's a bug, you should send me your
>   debug.log. (which is at ~/.bitcoin/debug.log)
>
>
>   The system tray in Gnome is not very reliable. Sometimes an icon
>   will disappear leaving no way to get back to the program. I have
>   verified that this can happen with bitcoin. It would be nice if
>   starting bitcoin while it's already running would just bring up
>   the GUI of the already running bitcoin process.
>
>
>   We haven't figured out how to find and bring up the existing running
>   program yet on Linux like it does on Windows. Given what you say, I
>   should at least turn off the minimize to tray option initially by
>   default.
>
>

Email #67

Date: Sun, 08 Nov 2009 18:48:38 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

To: mmalmi@cc.hut.fi

I'm not really a fan of that type of forum layout. The thread list only fits about 4 threads on a page, posts are treated like news articles or blog posts with reply comments at the bottom. It's more of a social networking site, not really conducive to technical discussion.

I'm thinking phpBB or IPB or similar. One line of text per thread, small fonts, efficient use of vertical space. Most people are already familiar with the interface.

mmalmi@cc.hut.fi wrote:
> I made a ning.com site for testing: bitcoin.ning.com. At least it's
> there to get Google hits, even if we didn't use it.
>
>> Now that the forum on bitcoin.sourceforge.net is catching on, we really
>> should look for somewhere that freehosts full blown forum software.
>> The bitweaver forum feature is just too lightweight. I assume the
>> "Forum" tab on the homepage can link out to wherever the forum is
>> hosted.
>>
>> I've seen projects that have major following just from forum talk and
>> pie-in-the-sky planning without even having any code yet. Having a lot
>> of forum talk gives a project more presence on the net, more search
>> hits, makes it look big, draws new users in, helps solve support
>> questions, hashes out what features are most of wanted.
>>
>> It would be a big plus if it could support SSL, at least for the login
>> page if not sitewide. Multiple people on the forum have expressed
>> interest in TOR/I2P, and those users need SSL because a lot of TOR exit
>> nodes are probably password scrapers run by identity thieves. A lot of
>> the core interest in Bitcoin is going to be from the privacy crowd.
>>
>> Any ideas where we can get a free forum? Maybe we should look at where
>> some other projects have their forums hosted for ideas where to look.
>
>

>

Email #68

Date: Mon, 09 Nov 2009 01:23:59 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Linux build ready for testing
To: Liberty Standard <newlibertystandard@gmail.com>
Cc: Martti Malmi <mmalmi@cc.hut.fi>

Liberty Standard wrote:
> Ok, blocks have now started to increase. It definitely takes longer for
> them to start increasing than with the Windows version. Also, I think
> they might be increasing at a slower rate than in with the Windows
> version. Is there perhaps debugging enabled in the Linux build that you
> sent me? Block are increasing at about 15 blocks per second (eyeball
> estimate while looking at a clock). I didn't time how fast they
> increased in the Windows version, but it seems like it was much faster.

About how long did it take to start? It could be the node that you
happened to request from is slow. The slow start is consistent with the
slow download speed.

I'd like to look at your current debug.log file and try to understand
what's going. It might just be a really slow connection on the other
side, or maybe something's wrong and failed and retried. Taking too
long could confuse other users.

Martti, how long did it take to start downloading blocks when you ran
it, and how fast did it download?

> When I launch bitcoin and the bitcoin port is not available, I get
> the following messages to the command line. I don't get those
> messages when the bitcoin port is available. Would it be possible
> for bitcoin to pick another port if the default port is taken? The
> same think sometimes happens to me with my BitTorrent client. When I
> restart it, my previously open port is closed. All I have to do is
> change the port and it starts working again.
>
> /usr/lib/gio/modules/libgvfsdbus.so: wrong ELF class: ELFCLASS64
> Failed to load module: /usr/lib/gio/modules/libgvfsdbus.so
> /usr/lib/gio/modules/libgioremote-volume-monitor.so: wrong ELF

> class: ELFCLASS64
> Failed to load module:
> /usr/lib/gio/modules/libgioremote-volume-monitor.so
> /usr/lib/gio/modules/libgiogconf.so: wrong ELF class: ELFCLASS64
> Failed to load module: /usr/lib/gio/modules/libgiogconf.so

It already uses SO_REUSEADDR so it can bind to the port if it's in TIME_WAIT state after being closed. The only time it should fail to bind is when the program really is already running. It's important that two copies of Bitcoin not run on the same machine at once because they would be modifying the database at the same time. There is never any need to run two on one machine as coin generation will now use multiple processors automatically.

I'm not sure what those lib errors are, I'll do some searching.

Email #69

Date: Mon, 09 Nov 2009 05:42:59 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Linux build ready for testing
To: Liberty Standard <newlibertystandard@gmail.com>
Cc: Martti Malmi <mmalmi@cc.hut.fi>

Thanks for that, I see what happened. Because the first one was slow, it ended up requesting the blocks from everybody else, which only bogged everything down. I can fix this, I just need to think a while about the right way.

There's no risk in shutting down while there are unconfirmed. When you make a transaction or new block, it immediately broadcasts it to the network. After that, the increasing #/confirmed number is just monitoring the outcome. There's nothing your node does during that time to promote the acceptance.

Now that I think about it, when you close Bitcoin, it closes the main window immediately but in the background continues running to finish an orderly flush and shutdown of the database. Before I implemented that, it was annoying having a dead hung unresponsive window hanging around. Until it finishes the orderly shutdown in the background, the port would be locked, and this is an important protection to make sure another copy can't touch the database until it's done. I haven't seen the shutdown take more than a few seconds.

In Wine, there's no way for the Windows version to do SO_REUSEADDR, so that would add 60 seconds (on my system) of TIME_WAIT after the port is closed.

If you need to transfer between two copies, you could send it to the other's bitcoin address. The receiving copy doesn't have to be online at the time.

The command line to use a different data directory is
bitcoin -datadir=<directory>

For example, on Linux, the default directory is (don't use ~)
bitcoin -datadir=/home/yourusername/.bitcoin

You shouldn't normally have any need to use this switch. It still won't let you run two instances at once.

Liberty Standard wrote:
> On Mon, Nov 9, 2009 at 3:23 AM, Satoshi Nakamoto <satoshin@gmx.com
> <mailto:satoshin@gmx.com>> wrote:
>
> Liberty Standard wrote:
>
> Ok, blocks have now started to increase. It definitely takes
> longer for them to start increasing than with the Windows
> version. Also, I think they might be increasing at a slower rate
> than in with the Windows version. Is there perhaps debugging
> enabled in the Linux build that you sent me? Block are
> increasing at about 15 blocks per second (eyeball estimate while
> looking at a clock). I didn't time how fast they increased in
> the Windows version, but it seems like it was much faster.
>
>
> About how long did it take to start? It could be the node that you
> happened to request from is slow. The slow start is consistent with
> the slow download speed.
>
>
> It took about a half hour for it to start incrementing quickly.
> Interestingly, the CPU usage increased before it started to increment
> steadily and then lowered when it started to increment steadily.
> Although this time the block incremented to 2 within the first few

> minutes. I have not yet generated any bitcoins. I'll wait for as long as
> I have patience to generate a bitcoin, but if none are created by the
> time I lose patience, I'm going to move back to the wine version.
>
> I'd like to look at your current debug.log file and try to
> understand what's going. It might just be a really slow connection
> on the other side, or maybe something's wrong and failed and
> retried. Taking too long could confuse other users.
>
>
> I've included my current debug.log.
>
>
> Martti, how long did it take to start downloading blocks when you
> ran it, and how fast did it download?
>
>
> When I launch bitcoin and the bitcoin port is not available,
> I get
> the following messages to the command line. I don't get those
> messages when the bitcoin port is available. Would it be possible
> for bitcoin to pick another port if the default port is
> taken? The
> same think sometimes happens to me with my BitTorrent client.
> When I
> restart it, my previously open port is closed. All I have to
> do is
> change the port and it starts working again.
>
> /usr/lib/gio/modules/libgvfsdbus.so: wrong ELF class: ELFCLASS64
> Failed to load module: /usr/lib/gio/modules/libgvfsdbus.so
> /usr/lib/gio/modules/libgioremote-volume-monitor.so: wrong ELF
> class: ELFCLASS64
> Failed to load module:
> /usr/lib/gio/modules/libgioremote-volume-monitor.so
> /usr/lib/gio/modules/libgiogconf.so: wrong ELF class: ELFCLASS64
> Failed to load module: /usr/lib/gio/modules/libgiogconf.so
>
>
> It already uses SO_REUSEADDR so it can bind to the port if it's in
> TIME_WAIT state after being closed. The only time it should fail to
> bind is when the program really is already running. It's important
> that two copies of Bitcoin not run on the same machine at once

> because they would be modifying the database at the same time.
> There is never any need to run two on one machine as coin
> generation will now use multiple processors automatically.
>
>
> The reason I run two instances at the same time is to transfer bitcoins
> from one bitcoin instance to another. They of course would need to be
> accessing different data directories. Perhaps that could be specified as
> a command line argument. I currently have to move my bitcoin data folder
> to a virtual machine to do this. Shutting down bitcoin and restarting it
> with a different data directory is a poor solution because shutting down
> bitcoin while there are unconfirmed bitcoins risks losing those bitcoins.
>
> Bitcoin was definitely not running when i get the busy port error. The
> process closes quickly and reliably from my experience, but it takes
> anywhere from 30 seconds to 3 minutes (estimation from memory) for the
> port to become available again. It occurred while switching from bitcoin
> 0.1.5 in Wine to the Linux build and again while switching from the
> Linux build to bitcoin 0.1.5 in Wine.
>
> Another thing that I noticed is that the about dialog text does not fit
> correctly and it cannot be resized.
>
> I'm not sure what those lib errors are, I'll do some searching.
>
>

Email #70

Date: Mon, 09 Nov 2009 10:32:08 +0200
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Cc: Liberty Standard <newlibertystandard@gmail.com>
Subject: Re: Linux build ready for testing

> Martti, how long did it take to start downloading blocks when you ran
> it, and how fast did it download?

Started very quickly when I got connected and downloaded quicker than
my Windows PC, which has a slower CPU.

I'll have to focus on a school project (coincidentally C++ coding) for

about a month now, so I don't have that much time for active developing until December. Let's keep contact anyway.

> Liberty Standard wrote:
>> Ok, blocks have now started to increase. It definitely takes longer
>> for them to start increasing than with the Windows version. Also,
>> I think they might be increasing at a slower rate than in with the
>> Windows version. Is there perhaps debugging enabled in the Linux
>> build that you sent me? Block are increasing at about 15 blocks per
>> second (eyeball estimate while looking at a clock). I didn't time
>> how fast they increased in the Windows version, but it seems like
>> it was much faster.
>
> About how long did it take to start? It could be the node that you
> happened to request from is slow. The slow start is consistent with
> the slow download speed.
>
> I'd like to look at your current debug.log file and try to understand
> what's going. It might just be a really slow connection on the other
> side, or maybe something's wrong and failed and retried. Taking too
> long could confuse other users.
>
> Martti, how long did it take to start downloading blocks when you ran
> it, and how fast did it download?
>
>> When I launch bitcoin and the bitcoin port is not available, I get
>> the following messages to the command line. I don't get those
>> messages when the bitcoin port is available. Would it be possible
>> for bitcoin to pick another port if the default port is taken? The
>> same think sometimes happens to me with my BitTorrent client. When I
>> restart it, my previously open port is closed. All I have to do is
>> change the port and it starts working again.
>>
>> /usr/lib/gio/modules/libgvfsdbus.so: wrong ELF class: ELFCLASS64
>> Failed to load module: /usr/lib/gio/modules/libgvfsdbus.so
>> /usr/lib/gio/modules/libgioremote-volume-monitor.so: wrong ELF
>> class: ELFCLASS64
>> Failed to load module:
>> /usr/lib/gio/modules/libgioremote-volume-monitor.so
>> /usr/lib/gio/modules/libgiogconf.so: wrong ELF class: ELFCLASS64
>> Failed to load module: /usr/lib/gio/modules/libgiogconf.so
>
> It already uses SO_REUSEADDR so it can bind to the port if it's in

> TIME_WAIT state after being closed. The only time it should fail to
> bind is when the program really is already running. It's important
> that two copies of Bitcoin not run on the same machine at once because
> they would be modifying the database at the same time. There is never
> any need to run two on one machine as coin generation will now use
> multiple processors automatically.
>
> I'm not sure what those lib errors are, I'll do some searching.

Email #71

Date: Mon, 09 Nov 2009 19:30:53 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build ready for testing

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

You really don't want to keep running in Wine, you're getting database errors (db.log). You probably developed these rituals of transferring to a fresh install to cope with database corruption. If there is a way to lose unconfirmed blocks, it would have to be the database errors. Any problems you find in the Linux build can be fixed. The Wine incompatibility deep inside Berkeley DB is unfixable.

I think GCC 4.3.3 on the Linux build optimized the SHA-256 code better than the old GCC 3.4.5 on Windows. When I was looking for the best SHA-256 code, there was a lot of hand tuned highly optimized SHA1 code available, but not so much for SHA-256 yet. I should see if I can upgrade MinGW to 4.3.x to get them on a level playing field.

Liberty Standard wrote:
> Everyone that contributed to making this Linux build really did a great
> job! Thanks for the hard work. It has started maturing some bitcoins, so
> I'm going to continue to run the Linux client for the time being until I
> decide whether it's at least as good or better at generating coins than
> the Windows version running in Wine.
>
>
> On Mon, Nov 9, 2009 at 8:59 AM, Liberty Standard
> <newlibertystandard@gmail.com <mailto:newlibertystandard@gmail.com>> wrote:

> Another instance when I would like to run multiple instances is when
> I upgrade bitcoin. I will uncheck the generate coin check box in the
> outdated bitcoin, launch and start generating coins in the new
> bitcoin using a separate data directory, then when the old
> application's coins have matured I will send them to the new
> application and then close the old application. I prefer do do clean
> installs rather than upgrading while maintaining old data.
>
>
>
> On Mon, Nov 9, 2009 at 7:42 AM, Satoshi Nakamoto <satoshin@gmx.com
> <mailto:satoshin@gmx.com>> wrote:
>
> Thanks for that, I see what happened. Because the first one was
> slow, it ended up requesting the blocks from everybody else,
> which only bogged everything down. I can fix this, I just need
> to think a while about the right way.
>
> There's no risk in shutting down while there are unconfirmed.
> When you make a transaction or new block, it immediately
> broadcasts it to the network. After that, the increasing
> #/confirmed number is just monitoring the outcome. There's
> nothing your node does during that time to promote the acceptance.
>

Email #72

Date: Mon, 09 Nov 2009 19:41:11 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build ready for testing

To: mmalmi@cc.hut.fi

Cc: Liberty Standard <newlibertystandard@gmail.com>

You got a lot done with the Linux build, autostart, minimize to tray,
setup and everything, it's really appreciated. Good luck on your C++
project.

mmalmi@cc.hut.fi wrote:
> I'll have to focus on a school project (coincidentally C++ coding) for
> about a month now, so I don't have that much time for active developing

> until December. Let's keep contact anyway.
>

Email #73

Date: Tue, 10 Nov 2009 16:46:04 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Linux - dead sockets problem
To: Liberty Standard <newlibertystandard@gmail.com>
Cc: Martti Malmi <mmalmi@cc.hut.fi>

I see what happened. All your sockets went dead somehow. You had no communication with the network, but because you had 8 zombie connections, it thought it was still online and kept generating blocks.
You can tell this is happening when your blocks are numbered sequentially, without other people's blocks interspersed, like:
2/unconfirmed
3/unconfirmed
4/unconfirmed
5/unconfirmed
6 blocks
7 blocks

It's implausible that you would be the only one to find blocks for 6 blocks in a row like that.

When you exited and restarted, it connected and downloaded 45 blocks that the network found in your absence. Since your blocks were not broadcast to the network immediately, the network went on without them.

It sounds like you had exactly the same problem on Wine. There's clearly something about socket handling on Linux that's effecting it either way.

I'll start researching this. Ultimately if I can't find the root of the problem, I'll have to make some kind of mechanism to watch for an absence of messages and disconnect. The only workaround for you right now would be to exit and restart more often.

All but one of your node connections went dead at the same time, one shortly after. IRC was still working, so it wasn't that you were offline from the internet.

I wonder if the status of blocks should say "#/unconfirmed" all the way up to maturity (119/unconfirmed then 120 blocks) instead. The meaning of the number isn't as strong for blocks as for transactions.

I think it would be an improvement not to count one's own blocks as confirmations. A drawback would be that the status numbers shown by different nodes would not match. The status number would no longer be coordinated with the maturity countdown on blocks either. A lighter option would be a special case only if all confirmations are your own.

Liberty Standard wrote:
> I just lost 6 sets of maturing coins! I had 10 sets of bitcoins
> maturing. The last set was generated at about 0:22. It got to
> 2/unconfirmed before bitcoin got stuck. At 10:10, the bitcoin which was
> generated at 0:22 was still only at 2/unconfirmed. Since you had told me
> that I wasn't going to lose coins, I shutdown and restarted bitcoin. On
> the bright side, it shutdown and started up very smoothly. But
> unfortunately, when the blocks updated, I lost 6 sets of bitcoins. Four
> sets were still unconfirmed, but two sets were confirmed. And there's no
> trace of them now. Perhaps now that you have the 'Show Generated Coins'
> option available, you can put back in failed bitcoin generations. I just
> don't like that those bitcoins just disappeared into thin air. I'm still
> running the Linux build at the moment, but the Wine version is suddenly
> looking much more attractive now that 6 out of the 10 sets of bitcoins I
> generated in the past 24 hours just vanished. I've included my debug.log.
>
>
> On Tue, Nov 10, 2009 at 1:45 AM, Liberty Standard
> <newlibertystandard@gmail.com <mailto:newlibertystandard@gmail.com>> wrote:
>
>   The Linux build has generated a decent amount of bitcoins within the
>   past 20 hours and I trust what you're telling me about database
>   errors, so all signs point toward me running the Linux build from
>   now on. The only half annoying thing about the Linux build is that
>   my computer's fan has gone from 50% to 100%. :-P I know I can limit
>   the CPU, so if it gets on my nerves too much and if I can live with
>   less bitcoins being generated, perhaps I'll do that. Or maybe I just
>   need to start listening to more music...
>
...
>
>   There's no risk in shutting down while there are
>   unconfirmed.

> When you make a transaction or new block, it immediately
> broadcasts it to the network. After that, the increasing
> #/confirmed number is just monitoring the outcome.
> There's
> nothing your node does during that time to promote
> the acceptance.
>
>
>

Email #74

Date: Wed, 11 Nov 2009 00:39:19 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux - linux-0.1.6-test2

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

I fixed a few places I found where it was possible for a socket to get
an error and not get disconnected. If your connections go dead again,
it should disconnect and reconnect them. I also implemented an
inactivity timeout as a fallback.

This also includes a partial fix for the slow initial block download.

You should run with the "-debug" switch to get some additional debug.log
information I added that'll help if there are more problems.

linux-0.1.6-test2.tar.bz2 12,134,012 bytes
Download:
http://rapidshare.com/files/305231818/linux-0.1.6-test2.tar.bz2.html

Satoshi Nakamoto wrote:
> I see what happened. All your sockets went dead somehow. You had no
> communication with the network, but because you had 8 zombie
> connections, it thought it was still online and kept generating blocks.
> You can tell this is happening when your blocks are numbered
> sequentially, without other people's blocks interspersed, like:
> 2/unconfirmed
> 3/unconfirmed
> 4/unconfirmed

> 5/unconfirmed
> 6 blocks
> 7 blocks
>
> It's implausible that you would be the only one to find blocks for 6
> blocks in a row like that.
>
> When you exited and restarted, it connected and downloaded 45 blocks
> that the network found in your absence. Since your blocks were not
> broadcast to the network immediately, the network went on without them.
>
> It sounds like you had exactly the same problem on Wine. There's
> clearly something about socket handling on Linux that's effecting it
> either way.
>
> I'll start researching this. Ultimately if I can't find the root of the
> problem, I'll have to make some kind of mechanism to watch for an
> absence of messages and disconnect. The only workaround for you right
> now would be to exit and restart more often.
>
> All but one of your node connections went dead at the same time, one
> shortly after. IRC was still working, so it wasn't that you were
> offline from the internet.
>
> I wonder if the status of blocks should say "#/unconfirmed" all the way
> up to maturity (119/unconfirmed then 120 blocks) instead. The meaning
> of the number isn't as strong for blocks as for transactions.
>
> I think it would be an improvement not to count one's own blocks as
> confirmations. A drawback would be that the status numbers shown by
> different nodes would not match. The status number would no longer be
> coordinated with the maturity countdown on blocks either. A lighter
> option would be a special case only if all confirmations are your own.
>
> Liberty Standard wrote:
>> I just lost 6 sets of maturing coins! I had 10 sets of bitcoins
>> maturing. The last set was generated at about 0:22. It got to
>> 2/unconfirmed before bitcoin got stuck. At 10:10, the bitcoin which
>> was generated at 0:22 was still only at 2/unconfirmed. Since you had
>> told me that I wasn't going to lose coins, I shutdown and restarted
>> bitcoin. On the bright side, it shutdown and started up very smoothly.
>> But unfortunately, when the blocks updated, I lost 6 sets of bitcoins.
>> Four sets were still unconfirmed, but two sets were confirmed. And

>> there's no trace of them now. Perhaps now that you have the 'Show
>> Generated Coins' option available, you can put back in failed bitcoin
>> generations. I just don't like that those bitcoins just disappeared
>> into thin air. I'm still running the Linux build at the moment, but
>> the Wine version is suddenly looking much more attractive now that 6
>> out of the 10 sets of bitcoins I generated in the past 24 hours just
>> vanished. I've included my debug.log.
>>
>>
>> On Tue, Nov 10, 2009 at 1:45 AM, Liberty Standard
>> <newlibertystandard@gmail.com <mailto:newlibertystandard@gmail.com>>
>> wrote:
>>
>>   The Linux build has generated a decent amount of bitcoins within the
>>   past 20 hours and I trust what you're telling me about database
>>   errors, so all signs point toward me running the Linux build from
>>   now on. The only half annoying thing about the Linux build is that
>>   my computer's fan has gone from 50% to 100%. :-P I know I can limit
>>   the CPU, so if it gets on my nerves too much and if I can live with
>>   less bitcoins being generated, perhaps I'll do that. Or maybe I just
>>   need to start listening to more music...
>>
> ...
>>
>>   There's no risk in shutting down while there are
>>   unconfirmed.
>>   When you make a transaction or new block, it
>> immediately
>>   broadcasts it to the network. After that, the
>> increasing
>>   #/confirmed number is just monitoring the outcome.
>>   There's
>>   nothing your node does during that time to promote
>>   the acceptance.
>>
>>
>>
>>
>
>

Email #75

Date: Wed, 11 Nov 2009 00:41:06 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux - linux-0.1.6-test2 attachment

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

linux-0.1.6-test2.tar.bz2 attached

Email #76

Date: Thu, 12 Nov 2009 05:36:06 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Linux - linux-0.1.6-test3

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

Right now (04:50 GMT) my node is connecting to yours and getting zombie connections each time. The socket isn't returning an error, just zombie without notice. If you're running the linux build right now, it would be interesting to see what the log says on your side.

test3:

I've added specific code to detect zombie sockets. It'll detect if the socket hasn't sent or received any data within 60 seconds of connecting, and detect if data is queued to send and hasn't sent for 3 minutes.

I think I may have weakened the reconnect speed in test2. In test3 I'm making it more determined to reconnect quickly.

I added checking to track whether other nodes received your generated blocks. If none did, it'll warn you in the description:
"Generated - Warning: This block was not received by any other nodes and will probably not be accepted!"

The status can go to "#/offline?" for blocks or transactions you create if they don't get out to any other nodes.

With all this, it should be impossible not to notice as soon as it screws up. It should hopefully disconnect all the zombie sockets. After that, whether it's able to make some good connections, or sockets

is completely hosed and it stays at 0 connections, I don't know.

If this doesn't work, I guess I'll look at the sourcecode of some other P2P apps like BitTorrent and see how they deal with this stuff. Maybe there's some magic flag or procedure to bash the sockets system back to life.

File linux-0.1.6-test3.tar.bz2 attached in the next message.

Liberty Standard wrote:
> On Wed, Nov 11, 2009 at 8:08 AM, Liberty Standard
> <newlibertystandard@gmail.com <mailto:newlibertystandard@gmail.com>> wrote:
>
> My network connection is direct to my computer. My ISP requires that
> I run VPN to connect to the Internet. I then have a second NIC that
> shares my Internet with other devices. My IP address while using my
> computer is my actual IP address, but the devices connected through
> my second NIC use NAT. When I connect through a virtual machine,
> that also uses NAT. All this requires very little configuration.
> NetworkManager in Ubuntu has an option to share my Internet
> connection through the second NIC and VirtualBox has the option to
> use NAT.
>
> I lost a couple packs of bitcoins again, so that problem is not yet
> fixed. It's a bit more bearable now that I have an idea of what is
> going on. I figure for now I'll just restart bitcoin whenever I see
> a pack of bitcoins starting to mature. I may go back and forth a bit
> between Linux and Wine, but I'll definitely test every new version
> that comes out. At the moment I'm still running the Linux build.
>
>
>
> On Wed, Nov 11, 2009 at 7:49 AM, Satoshi Nakamoto <satoshin@gmx.com
> <mailto:satoshin@gmx.com>> wrote:
>
> Thanks. The log didn't stop on anything special, just simple
> message passing. Chances are it's UI related. Most of the
> initial bugs were all UI.
>
> What brand/model of firewall do you have? It's possible for
> BitTorrent to overwhelm the number of connections some models
> can handle. Most are underpowered and flaky under load.

>
> NewLibertyStandard wrote:
>
> I have been getting your attachments just fine. I just
> thought I'd spare Martti the large attachment.
>
> I am not able to reproduce the bug. I don't know whether the
> paste, the blocks finishing, a combination of the two or
> something else entirely caused the fault.
>
> ...
>
> But after they started
> downloading, I took a look a look at my BitTorrent
> client, and
> sure enough, I had forgotten about a torrent and my
> upload was
> quite high, at the limit I had set for it.
>
>
>
>
>

Email #77

Date: Thu, 12 Nov 2009 05:37:58 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: linux-0.1.6-test3.tar.bz2 attached

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

File linux-0.1.6-test3.tar.bz2 attached

linux-0.1.6-test3.tar.bz2 12,143,473 bytes

Email #78

Date: Thu, 12 Nov 2009 23:39:44 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: linux-0.1.6-test5 fix for zombie sockets

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

test 5:

I added MSG_DONTWAIT to the send and recv calls in case they forgot the socket is non-blocking. If that doesn't work, there's now the catch-all solution: another thread monitors the send/recv thread and terminates and restarts it if it stops. It prints "*** Restarting ThreadSocketHandler ***" in debug.log, and an error message displays on the status bar for a while.

Before terminating, it tries closing the socket that's hung. If that works, it doesn't have to resort to terminating.

I ran a test where it terminated the thread about 1000 times without trouble, so it should be safe. The terminate on linux is pthread_cancel, which throws it into C++'s exception handler.

The thread calls we were using didn't have terminate, so I created our own wrappers in util.h to use CreateThread on windows and pthread_create on linux, instead of:

- _beginthread is windows only and lacks terminate
- boost::thread is really attractive, but lacks terminate
- wxThread requires you to create a class for every function you might call (yuck)

File attached in the next e-mail

Email #79

Date: Thu, 12 Nov 2009 23:42:29 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: linux-0.1.6-test5.tar.bz2 attached

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

12,033,918 linux-0.1.6-test5.tar.bz2

Email #80

Date: Sat, 14 Nov 2009 05:46:22 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Zetaboards forum

To: Martti Malmi <mmalmi@cc.hut.fi>

I created a forum on Zetaboards, InvisionFree's new site that they're migrating to.

http://s1.zetaboards.com/Bitcoin/index/

I made an admin account you can use to upgrade your own account to admin:
u: admin
pw: B98VzUUA

BTW, the admin pages have a huge blank space at the top, you have to scroll down.

It doesn't support SSL, but none of them do. I replaced the ugly default orange and blue theme with the Frostee theme, which was the only decent looking theme I could find after extensive searching. Searching for themes is futile, there are thousands of rubbish themes. It turns out the solution is to look at button sets instead (http://resources.zetaboards.com/forum/1000328/)

I only created two subforums to begin with. I'll create new ones as the need arises. I like to start with a flat namespace until there's enough items to justify subsections. Technical Support makes sense as a separate section to get that stuff out of the main spotlight so our dirty laundry isn't in everyone's face, and to make people feel more free to report bugs there. Mostly only devs and people checking on a bug need read the Technical Support section.

Email #81

Date: Sun, 15 Nov 2009 15:40:29 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Linux update

To: Martti Malmi <mmalmi@cc.hut.fi>

linux-0.1.6-test5 solved Liberty's zombie socket problem. The MSG_DONTWAIT fixed the root cause, it's not having to terminate and restart the thread. The sockets are marked non-blocking already, so I don't understand why. Maybe it forgot. I suppose if a socket fails and the OS closes it then there's nothing left to remember it was non-blocking, but then accessing a closed handle should return immediately with an error. There's no MSG_DONTWAIT on Windows, marking the socket as nonblocking is the only way, so if anyone runs the Windows version in Wine it will have to rely on terminating the thread.

The only problem now is the DB exceptions he's getting.

```
**********
EXCEPTION: 11DbException
Db::open: Bad file descriptor
bitcoin in ThreadMessageHandler()
**********
EXCEPTION: 11DbException
Db::close: Bad file descriptor
bitcoin in ThreadMessageHandler()
```

I had expected those to be a Wine problem, but he's getting them on Linux just the same. He tried moving the datadir to a different drive, no help. I've never gotten them. I'm running a stress test that continuously generates a lot of activity and DB access and never got it.

He has Ubuntu 64-bit and I have 32-bit, so I'm assuming that's the difference. Is your Linux machine 64-bit or 32-bit? Have you ever had a DB exception? (see db.log also) Now that the zombie problem is fixed in test5, could you start running it on your Linux machine? We could use a 3rd vote to get a better idea of what we're dealing with here. The DB exception is uncaught, so it'll stop the program if you get it.

BTW, zetaboards insists on displaying "Member #", so you better sign up soon and grab a good account number.

Email #82

Date: Sun, 15 Nov 2009 19:55:35 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux update

The program terminated a few times with the same error in debug.log
close: Bad file descriptor
blkindex.dat: Bad file descriptor

I'm running a 64-bit Ubuntu distribution.

> The only problem now is the DB exceptions he's getting.
> **********
> EXCEPTION: 11DbException
> Db::open: Bad file descriptor
> bitcoin in ThreadMessageHandler()
> **********
> EXCEPTION: 11DbException
> Db::close: Bad file descriptor
> bitcoin in ThreadMessageHandler()
>
> I had expected those to be a Wine problem, but he's getting them on
> Linux just the same. He tried moving the datadir to a different drive,
> no help. I've never gotten them. I'm running a stress test that
> continuously generates a lot of activity and DB access and never got it.
>
> He has Ubuntu 64-bit and I have 32-bit, so I'm assuming that's the
> difference. Is your Linux machine 64-bit or 32-bit? Have you ever had
> a DB exception? (see db.log also) Now that the zombie problem is fixed
> in test5, could you start running it on your Linux machine? We could
> use a 3rd vote to get a better idea of what we're dealing with here.
> The DB exception is uncaught, so it'll stop the program if you get it.
>
> BTW, zetaboards insists on displaying "Member #", so you better sign up
> soon and grab a good account number.

Email #83

Date: Sun, 15 Nov 2009 19:15:42 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux update

To: mmalmi@cc.hut.fi

I'd better install 64-bit then. I imagine it's something about the
32-bit version of Berkeley DB on 64-bit Linux.

BTW, in things like the feature list credits, do you want me to refer to
you as sirius-m or Martti Malmi? I think most projects go by real names
for consistency.

mmalmi@cc.hut.fi wrote:
> The program terminated a few times with the same error in debug.log from
> Db::close. Db.log has:
>
> close: Bad file descriptor
> blkindex.dat: Bad file descriptor
>
> I'm running a 64-bit Ubuntu distribution.
>
>> The only problem now is the DB exceptions he's getting.
>> **********
>> EXCEPTION: 11DbException
>> Db::open: Bad file descriptor
>> bitcoin in ThreadMessageHandler()
>> **********
>> EXCEPTION: 11DbException
>> Db::close: Bad file descriptor
>> bitcoin in ThreadMessageHandler()
>>
>> I had expected those to be a Wine problem, but he's getting them on
>> Linux just the same. He tried moving the datadir to a different drive,
>> no help. I've never gotten them. I'm running a stress test that
>> continuously generates a lot of activity and DB access and never got it.
>>
>> He has Ubuntu 64-bit and I have 32-bit, so I'm assuming that's the
>> difference. Is your Linux machine 64-bit or 32-bit? Have you ever had
>> a DB exception? (see db.log also) Now that the zombie problem is fixed
>> in test5, could you start running it on your Linux machine? We could
>> use a 3rd vote to get a better idea of what we're dealing with here.
>> The DB exception is uncaught, so it'll stop the program if you get it.
>>
>> BTW, zetaboards insists on displaying "Member #", so you better sign up
>> soon and grab a good account number.
>

Email #84

Date: Sun, 15 Nov 2009 22:05:50 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux update

Perhaps the real name is better.

Another name question: I've been thinking of a name for the exchange service, and I came up with Bitcoin X (bitcoinx.com) and Bitcoin Shop (bitcoinshop.com). Which one do you find better?

> I'd better install 64-bit then. I imagine it's something about the
> 32-bit version of Berkeley DB on 64-bit Linux.
>
> BTW, in things like the feature list credits, do you want me to refer
> to you as sirius-m or Martti Malmi? I think most projects go by real
> names for consistency.
>
> mmalmi@cc.hut.fi wrote:
>> The program terminated a few times with the same error in debug.log
>> from Db::close. Db.log has:
>>
>> close: Bad file descriptor
>> blkindex.dat: Bad file descriptor
>>
>> I'm running a 64-bit Ubuntu distribution.
>>
>>> The only problem now is the DB exceptions he's getting.
>>> **********
>>> EXCEPTION: 11DbException
>>> Db::open: Bad file descriptor
>>> bitcoin in ThreadMessageHandler()
>>> **********
>>> EXCEPTION: 11DbException
>>> Db::close: Bad file descriptor
>>> bitcoin in ThreadMessageHandler()
>>>
>>> I had expected those to be a Wine problem, but he's getting them on
>>> Linux just the same. He tried moving the datadir to a different drive,
>>> no help. I've never gotten them. I'm running a stress test that
>>> continuously generates a lot of activity and DB access and never got it.

>>>
>>> He has Ubuntu 64-bit and I have 32-bit, so I'm assuming that's the
>>> difference. Is your Linux machine 64-bit or 32-bit? Have you ever had
>>> a DB exception? (see db.log also) Now that the zombie problem is fixed
>>> in test5, could you start running it on your Linux machine? We could
>>> use a 3rd vote to get a better idea of what we're dealing with here.
>>> The DB exception is uncaught, so it'll stop the program if you get it.
>>>
>>> BTW, zetaboards insists on displaying "Member #", so you better sign up
>>> soon and grab a good account number.
>>

Email #85

Date: Sun, 15 Nov 2009 20:25:26 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Linux update
To: mmalmi@cc.hut.fi

At first glance, bitcoinshop.com looks better. bitcoinexchange.com
might be better than bitcoinx.com.

Be careful where you search domain names, many will front-run you. Even
network solutions, although they've said they won't if you use their
whois page not the homepage. The only safe place is
http://www.internic.com/whois.html

mmalmi@cc.hut.fi wrote:
> Perhaps the real name is better.
>
> Another name question: I've been thinking of a name for the exchange
> service, and I came up with Bitcoin X (bitcoinx.com) and Bitcoin Shop
> (bitcoinshop.com). Which one do you find better?
>
>> I'd better install 64-bit then. I imagine it's something about the
>> 32-bit version of Berkeley DB on 64-bit Linux.
>>
>> BTW, in things like the feature list credits, do you want me to refer
>> to you as sirius-m or Martti Malmi? I think most projects go by real
>> names for consistency.

>>
>> mmalmi@cc.hut.fi wrote:
>>> The program terminated a few times with the same error in debug.log
>>> from Db::close. Db.log has:
>>>
>>> close: Bad file descriptor
>>> blkindex.dat: Bad file descriptor
>>>
>>> I'm running a 64-bit Ubuntu distribution.
>>>
>>>> The only problem now is the DB exceptions he's getting.
>>>> **********
>>>> EXCEPTION: 11DbException
>>>> Db::open: Bad file descriptor
>>>> bitcoin in ThreadMessageHandler()
>>>> **********
>>>> EXCEPTION: 11DbException
>>>> Db::close: Bad file descriptor
>>>> bitcoin in ThreadMessageHandler()
>>>>
>>>> I had expected those to be a Wine problem, but he's getting them on
>>>> Linux just the same. He tried moving the datadir to a different drive,
>>>> no help. I've never gotten them. I'm running a stress test that
>>>> continuously generates a lot of activity and DB access and never got
>>>> it.
>>>>
>>>> He has Ubuntu 64-bit and I have 32-bit, so I'm assuming that's the
>>>> difference. Is your Linux machine 64-bit or 32-bit? Have you ever had
>>>> a DB exception? (see db.log also) Now that the zombie problem is fixed
>>>> in test5, could you start running it on your Linux machine? We could
>>>> use a 3rd vote to get a better idea of what we're dealing with here.
>>>> The DB exception is uncaught, so it'll stop the program if you get it.
>>>>
>>>> BTW, zetaboards insists on displaying "Member #", so you better sign up
>>>> soon and grab a good account number.
>>>
>>
>
>

Email #86

Date: Mon, 16 Nov 2009 06:20:52 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Db::open/Db::close "Bad file descriptor" exception

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

I have an idea for a workaround, but it depends on what files the errors are on. If you've accumulated several errors in db.log, could you send it to me? (even if it's rather simple and boring) Is the file listed always blkindex.dat, or does it include addr.dat or wallet.dat too?

Liberty Standard wrote:
> I moved the data directory back to my SSD card and started bitcoin test
> 6. It encountered a segmentation fault today with Db::open in the log. I
> had changed the settings to only use one processor/core while I watched
> a 720p mkv movie. I noticed the segmentation fault after the film had ended.
>
> On Sun, Nov 15, 2009 at 12:45 AM, Satoshi Nakamoto <satoshin@gmx.com
> <mailto:satoshin@gmx.com>> wrote:
>
> Here's one where I linked Berkeley DB a different way. It's worth a
> try. Otherwise identical to test5.
>
> (Keep the datadir on the hard drive at least until you get it to
> fail the same way there. That has a fair chance of success.)
>
>

Email #87

Date: Mon, 16 Nov 2009 19:19:26 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Forum

I installed a TikiWiki on my VPS at 174.143.149.98. SSL is currently enabled with a self-signed certificate. Admin password is the same as in the Bitweaver. How about using this as the site platform? Maybe we can make bitcoin.org or at least bitcoin.sf.net point there?

Email #88

Date: Mon, 16 Nov 2009 19:34:56 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> I installed a TikiWiki on my VPS at 174.143.149.98. SSL is currently
> enabled with a self-signed certificate. Admin password is the same as in
> the Bitweaver. How about using this as the site platform? Maybe we can
> make bitcoin.org or at least bitcoin.sf.net point there?

What do you see as the benefits of switching the wiki?
Some I can think of:
  SSL
  get away from sourceforge's unreliable hosting
  everything not logged by sourceforge

The forum feature is about as weak as bitweaver. We need a full blown
forum software for that.

My priority right now is to get a forum going, either phpBB or similar.
  What do you think of the zetaboards option? Should we go ahead with that?

Email #89

Date: Mon, 16 Nov 2009 22:11:24 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

> What do you see as the benefits of switching the wiki?
> Some I can think of:
> SSL
> get away from sourceforge's unreliable hosting
> everything not logged by sourceforge

I think the biggest advantage is having a single site so you don't
need a separate account for the wiki and the forum, and the
functionalities are also nicely integrated with the main site itself.

Also being ad-free is a plus.

> The forum feature is about as weak as bitweaver. We need a full blown
> forum software for that.

How about Drupal's forum functionality? Address:
https://174.143.149.98/drupal/. The CMS in general looks better and
simpler than TikiWiki. If the forum's not good enough, then we can of
course use a specialized forum software like phpBB.

> My priority right now is to get a forum going, either phpBB or similar.
> What do you think of the zetaboards option? Should we go ahead with
> that?

Otherwise fine, but the ads and the lack of SSL are a minus.

Email #90

Date: Mon, 16 Nov 2009 21:10:22 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

To: mmalmi@cc.hut.fi

That's a good idea to go in a more web-publishing CMS type direction
like Drupal. That's a better fit and can produce a better looking
website than a wiki. I think I was wrong about wiki. Only a few
specific people will do any website design work and those people can go
ahead and have a separate login. In that case, login integration with
the forum doesn't matter much. For security, I'd almost rather have a
different login than be constantly checking the forum with the same
login that could pwn the website.

Drupal's forum is less bad than the wikis, but still a long way from
something I would want to use.

zetaboards pros and cons:

pros:
- we don't have to worry about bandwidth
- they handle the backend management and security patches

con:

- lack of SSL
- lack of privacy, everything is logged
- lack of control over the php code for customization
- no CAPTCHA, and if they add one later it might be unacceptable flash
- ads (could pay to get rid of them later if we care enough)
- there's always the risk they abruptly cancel the site for some petty reason

mmalmi@cc.hut.fi wrote:
>> What do you see as the benefits of switching the wiki?
>> Some I can think of:
>> SSL
>> get away from sourceforge's unreliable hosting
>> everything not logged by sourceforge
>
> I think the biggest advantage is having a single site so you don't need
> a separate account for the wiki and the forum, and the functionalities
> are also nicely integrated with the main site itself. Also being ad-free
> is a plus.
>
>> The forum feature is about as weak as bitweaver. We need a full blown
>> forum software for that.
>
> How about Drupal's forum functionality? Address:
> https://174.143.149.98/drupal/. The CMS in general looks better and
> simpler than TikiWiki. If the forum's not good enough, then we can of
> course use a specialized forum software like phpBB.
>
>> My priority right now is to get a forum going, either phpBB or similar.
>> What do you think of the zetaboards option? Should we go ahead with
>> that?
>
> Otherwise fine, but the ads and the lack of SSL are a minus.
>

Email #91

Date: Tue, 17 Nov 2009 03:41:26 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: linux-0.1.6-test7

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

test 7:

Backup your data directory before running this, just in case.

Workaround for the Db::open/Db::close "Bad file descriptor" exception.
Might also make the initial block download faster. The workaround is to
open the database handles and keep them open for the duration of the
program, which is actually the more common thing to do anyway. If we're
not closing and opening all the time, the error shouldn't get a chance
to happen.

The one exception is wallet.dat, which I still close after writing is
finished so I can flush the transaction logs into the dat file, making
the dat file standalone. That way if someone does a backup while
Bitcoin is running, they'll get a wallet.dat that is valid by itself
without the database transaction logs.

This is a restructuring of the database handling, so we might find some
new deadlocks. Usually if it deadlocks, either the UI will stop
repainting, or it'll stop using CPU even though it still says Generating.

Email #92

Date: Tue, 17 Nov 2009 16:57:26 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> How about Drupal's forum functionality? Address:
> https://174.143.149.98/drupal/. The CMS in general looks better and
> simpler than TikiWiki. If the forum's not good enough, then we can of
> course use a specialized forum software like phpBB.

Another issue I thought of with zetaboards: most free forum sites won't
let you export the user account database if you want to move. I don't
know why I don't see any other software projects using a free forum, but
I have to assume there might be a reason we would discover later.

If you can install phpBB3 on your VPS, that's probably the better option.

From what I've seen on other forums, if the cost of bandwidth becomes an issue, a small Google Adwords (text links) at the top generates more than the cost of bandwidth even for very low value traffic like gaming. This would be much higher value traffic well targeted for high paying gold merchant keywords and VPN hosts. It could eventually be a valuable revenue stream you wouldn't want to give away to some free site.

I want to pre-announce some of the features in version 0.2 on the forum and try to get some anticipation going. Even if hardly anyone else is posting, I have seen project forums where most of the posts are the author announcing what's going on with the latest changes. Users can see progress going on, see that it's improving and supported and not abandonware. It's a little like a blog in that case, but easier for users to use it as a searchable FAQ and better organized. Whenever I google search software questions, most of the hits are forum posts.

Email #93

Date: Wed, 18 Nov 2009 03:31:39 +0200
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Forum

I installed both phpBB3 and Simple Machines Forum, which are kind of the market leaders among the open source forums. SMF's interface looks better on the first look, especially the admin panel. What do you think, shall we go with SMF or phpBB3?

Email #94

Date: Wed, 18 Nov 2009 03:50:24 +0200
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Db::open/Db::close "Bad file descriptor" exception

Here's the logs in case they're still useful.

> I have an idea for a workaround, but it depends on what files the
> errors are on. If you've accumulated several errors in db.log, could
> you send it to me? (even if it's rather simple and boring) Is the file
> listed always blkindex.dat, or does it include addr.dat or wallet.dat
> too?

Email #95

Date: Wed, 18 Nov 2009 04:35:32 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: linux-0.1.6-test7

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

Finally an easy one. I see a way that could happen on a long operation such as the initial download. The TryLock bug is unrelated to the db stuff. Fix will be in test8.

I've been able to reproduce the db::open/close exception 3 times now on 32-bit linux by hitting it with a continuous flood of non-stop requests. It looks like even periodically closing the wallet.dat database to flush it gets the db::close exceptions. I'm disabling the wallet flush feature on Linux. On Linux we'll never close a database handle until we're ready to exit. So far with this disabled, no exceptions.

I'm also implementing the orderly initial block download. Instead of naively requesting all the blocks at once, it'll request batches of 500 at a time. This way, it'll receive the blocks before the retry timeout, so it shouldn't go requesting it from other nodes unless it actually doesn't receive them or it's too slow. The change is in the requestee's side, so this functionality won't be visible until your initial block download is coming from a node that has the new version.

I'm going to test this some more before sending test8.

Liberty Standard wrote:
> I started with a fresh data directory with test7. Blocks started to
> download much faster. It only took about 15 seconds where it took a few
> minutes previously with the Linux build. It crashed once while it was
> downloading blocks with the following message in the terminal.
>
> ../include/wx/thrimpl.cpp(50): assert "m_internal" failed in TryLock():

> wxMutex::TryLock(): not initialized [in child thread]
> Trace/breakpoint trap
>
> I've included my log file, but I forgot to back it up before restarting
> bitcoin, so I'm not sure at what point in the log file the crash occurred.
>
> Fortunately I haven't encountered the segmentation fault yet. The
> frequency of segmentation faults in the previous builds varied quite a
> bit, so I'll keep running it and let you know if i run into any problems.
>
>
>
> On Tue, Nov 17, 2009 at 5:41 AM, Satoshi Nakamoto <satoshin@gmx.com
> <mailto:satoshin@gmx.com>> wrote:
>
>   test 7:
>
>   Backup your data directory before running this, just in case.
>
>   Workaround for the Db::open/Db::close "Bad file descriptor"
>   exception. Might also make the initial block download faster. The
>   workaround is to open the database handles and keep them open for
>   the duration of the program, which is actually the more common thing
>   to do anyway. If we're not closing and opening all the time, the
>   error shouldn't get a chance to happen.
>
>   The one exception is wallet.dat, which I still close after writing
>   is finished so I can flush the transaction logs into the dat file,
>   making the dat file standalone. That way if someone does a backup
>   while Bitcoin is running, they'll get a wallet.dat that is valid by
>   itself without the database transaction logs.
>
>   This is a restructuring of the database handling, so we might find
>   some new deadlocks. Usually if it deadlocks, either the UI will
>   stop repainting, or it'll stop using CPU even though it still says
>   Generating.
>
>

Email #96

Date: Wed, 18 Nov 2009 05:14:45 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Db::open/Db::close "Bad file descriptor" exception

To: mmalmi@cc.hut.fi

Thanks. The db::open/close errors confirm the pattern.

More interesting is the zombie sockets activity towards the end, and the socket thread monitor tripped but didn't get it going again. Was the machine disconnected from the net? MSG_DONTWAIT in test5 solved the zombie problem for Liberty. What test version were you running? (I should print the test version in the log)

mmalmi@cc.hut.fi wrote:
> Here's the logs in case they're still useful.
>
>> I have an idea for a workaround, but it depends on what files the
>> errors are on. If you've accumulated several errors in db.log, could
>> you send it to me? (even if it's rather simple and boring) Is the file
>> listed always blkindex.dat, or does it include addr.dat or wallet.dat
>> too?
>

Email #97

Date: Wed, 18 Nov 2009 05:32:22 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

To: mmalmi@cc.hut.fi

That's great, this is going to fun! I'll research what people say about the two.

mmalmi@cc.hut.fi wrote:
> I installed both phpBB3 and Simple Machines Forum, which are kind of
> the market leaders among the open source forums. SMF's interface looks
> better on the first look, especially the admin panel. What do you
> think, shall we go with SMF or phpBB3?
>
>

Email #98

Date: Wed, 18 Nov 2009 21:32:15 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Db::open/Db::close "Bad file descriptor" exception

I think it was test version 5, not completely sure though. I'm running
the Linux version on a laptop which I move between different locations
and use the hibernate-feature instead of powering down.

> Thanks. The db::open/close errors confirm the pattern.
>
> More interesting is the zombie sockets activity towards the end, and
> the socket thread monitor tripped but didn't get it going again. Was
> the machine disconnected from the net? MSG_DONTWAIT in test5 solved
> the zombie problem for Liberty. What test version were you running?
> (I should print the test version in the log)
>
> mmalmi@cc.hut.fi wrote:
>> Here's the logs in case they're still useful.
>>
>>> I have an idea for a workaround, but it depends on what files the
>>> errors are on. If you've accumulated several errors in db.log, could
>>> you send it to me? (even if it's rather simple and boring) Is the file
>>> listed always blkindex.dat, or does it include addr.dat or wallet.dat
>>> too?
>>

Email #99

Date: Fri, 20 Nov 2009 05:14:56 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: SMF forum, need a mod installed

To: Martti Malmi <mmalmi@cc.hut.fi>

I've been configuring the SMF forum. They're saying SMF is better
written than phpBB and more reliable, so if I can get SMF to look right,
that's the preferable choice.

Most forums run vBulletin (big-boards.com lists 1376 vBulletin, 275 Invision, 245 phpBB and 41 SMF), so if you don't look like vBulletin or Invision, it looks like you compromised because you couldn't afford vBulletin. SMF's UI started out further away from the standard look, but I've been able to use CSS to make it look more like the others.

I've done as much as I can with CSS, the rest requires editing PHP files and uploading images. The forum doesn't have a built in file upload/edit admin feature, it's added separately as the SMF File Manager mod. I uploaded the mod but some files need to be chmod 777 so it can install. If you go to Admin->Packages->Browse Packages and click on Apply Mod, it offers to do it automatically if you enter an ftp login.

Someone says you might also have to
mkdir /var/www/bitcoin/smf/packages/temp

The error in the error log is:
failed to open stream: Permission denied
File: /var/www/bitcoin/smf/Sources/Subs-Package.php
(I'm sure that's just the first file)

Is it OK to go live with this SMF installation when I'm finished configuring it? I should be able to point forum.bitcoin.org to it.

Liberty reports that linux-test8 has been running smoothly. My tests have been running fine as well. The Linux version looks fully stabilized to me.

Good news: he says he made his first sale of bitcoins. Someone bought out all he had. I had been wondering whether it would be buyers or sellers.

Email #100

Date: Fri, 20 Nov 2009 09:05:34 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

I don't have the time to configure it today, but I made a temporary account "maintenance" with password "6648ku5HeK" and full permissions

to /var/www/bitcoin. You can access it via ssh or sftp at port 30000.

It's okay to go live. Are you setting up a redirect or a dns entry? In case of dns entry I could set up an Apache vhost so that the forum address would be http://forum.bitcoin.org/.

Great that the Linux build works now. It's exciting to see how things will start rolling with the new release and the forum. Not too long until I can set up my own exchange and start promoting the currency to (web) business people.

NewLibertyStandard should perhaps change his pricing to the market price (i.e. what people are willing to buy and sell for) so that he doesn't run out of coins.

> I've been configuring the SMF forum. They're saying SMF is better
> written than phpBB and more reliable, so if I can get SMF to look
> right, that's the preferable choice.
>
> Most forums run vBulletin (big-boards.com lists 1376 vBulletin, 275
> Invision, 245 phpBB and 41 SMF), so if you don't look like vBulletin or
> Invision, it looks like you compromised because you couldn't afford
> vBulletin. SMF's UI started out further away from the standard look,
> but I've been able to use CSS to make it look more like the others.
>
> I've done as much as I can with CSS, the rest requires editing PHP
> files and uploading images. The forum doesn't have a built in file
> upload/edit admin feature, it's added separately as the SMF File
> Manager mod. I uploaded the mod but some files need to be chmod 777 so
> it can install. If you go to Admin->Packages->Browse Packages and
> click on Apply Mod, it offers to do it automatically if you enter an
> ftp login.
>
> Someone says you might also have to
> mkdir /var/www/bitcoin/smf/packages/temp
>
> The error in the error log is:
> failed to open stream: Permission denied
> File: /var/www/bitcoin/smf/Sources/Subs-Package.php
> (I'm sure that's just the first file)
>
> Is it OK to go live with this SMF installation when I'm finished
> configuring it? I should be able to point forum.bitcoin.org to it.

> Liberty reports that linux-test8 has been running smoothly. My tests
> have been running fine as well. The Linux version looks fully
> stabilized to me.
>
> Good news: he says he made his first sale of bitcoins. Someone bought
> out all he had. I had been wondering whether it would be buyers or
> sellers.

Email #101

Date: Fri, 20 Nov 2009 09:17:00 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

Oh yes, one more thing. I haven't configured the server's sendmail
yet, so the php mail functionality doesn't work, but it's not needed
yet anyway.

> I don't have the time to configure it today, but I made a temporary
> account "maintenance" with password "6648ku5HeK" and full permissions
> to /var/www/bitcoin. You can access it via ssh or sftp at port 30000.
>
> It's okay to go live. Are you setting up a redirect or a dns entry? In
> case of dns entry I could set up an Apache vhost so that the forum
> address would be http://forum.bitcoin.org/.
>
> Great that the Linux build works now. It's exciting to see how things
> will start rolling with the new release and the forum. Not too long
> until I can set up my own exchange and start promoting the currency to
> (web) business people.
>
> NewLibertyStandard should perhaps change his pricing to the market
> price (i.e. what people are willing to buy and sell for) so that he
> doesn't run out of coins.
>
>> I've been configuring the SMF forum. They're saying SMF is better
>> written than phpBB and more reliable, so if I can get SMF to look
>> right, that's the preferable choice.

>>
>> Most forums run vBulletin (big-boards.com lists 1376 vBulletin, 275
>> Invision, 245 phpBB and 41 SMF), so if you don't look like vBulletin or
>> Invision, it looks like you compromised because you couldn't afford
>> vBulletin. SMF's UI started out further away from the standard look,
>> but I've been able to use CSS to make it look more like the others.
>>
>> I've done as much as I can with CSS, the rest requires editing PHP
>> files and uploading images. The forum doesn't have a built in file
>> upload/edit admin feature, it's added separately as the SMF File
>> Manager mod. I uploaded the mod but some files need to be chmod 777 so
>> it can install. If you go to Admin->Packages->Browse Packages and
>> click on Apply Mod, it offers to do it automatically if you enter an
>> ftp login.
>>
>> Someone says you might also have to
>> mkdir /var/www/bitcoin/smf/packages/temp
>>
>> The error in the error log is:
>> failed to open stream: Permission denied
>> File: /var/www/bitcoin/smf/Sources/Subs-Package.php
>> (I'm sure that's just the first file)
>>
>> Is it OK to go live with this SMF installation when I'm finished
>> configuring it? I should be able to point forum.bitcoin.org to it.
>>
>> Liberty reports that linux-test8 has been running smoothly. My tests
>> have been running fine as well. The Linux version looks fully
>> stabilized to me.
>>
>> Good news: he says he made his first sale of bitcoins. Someone bought
>> out all he had. I had been wondering whether it would be buyers or
>> sellers.

Email #102

Date: Fri, 20 Nov 2009 22:09:41 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

To: mmalmi@cc.hut.fi

> It's okay to go live. Are you setting up a redirect or a dns entry? In
> case of dns entry I could set up an Apache vhost so that the forum
> address would be http://forum.bitcoin.org/.

DNS entry.

I'm thinking of merging the bitcoin.org information with your site content so I can switch the whole bitcoin.org domain over. We need to replace the current bitcoin.org site with a user-oriented site before the release.

If the website and forum switch at the same time, then forum.bitcoin.org isn't necessary unless we want it that way for looks.

Have you decided on the CMS to use? I should research Drupal and other CMSes and see what's the most popular.

> Great that the Linux build works now. It's exciting to see how things
> will start rolling with the new release and the forum. Not too long
> until I can set up my own exchange and start promoting the currency to
> (web) business people.

The linux version, setup exe, tor option and better website/forum will all increase the percentage of visitors who can use it, and the autostart and minimize to tray will increase how many keep running it. All those factors multiply together.

> NewLibertyStandard should perhaps change his pricing to the market price
> (i.e. what people are willing to buy and sell for) so that he doesn't
> run out of coins.

It's good to start low and only have the price go up.

I really like that he explains the concept that the cost of electricity is a minimum floor under the price. At a minimum you either have to pay the cost in electricity or pay someone the cost of production to make them for you.

Email #103

Date: Sat, 21 Nov 2009 07:02:20 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

To: mmalmi@cc.hut.fi

Thanks, that worked, I got File Manager installed with SSH. I also uploaded a few themes into Drupal. I haven't thoroughly gone through all the available themes yet.

Looked around at CMSes, Drupal and Joomla are popular. Consensus is Joomla has a better selection of themes and is easier to learn, though Drupal may be more intuitive for programmers and customization. Joomla better for CMS, Drupal better for blogs. Drupal's URLs are search engine friendly, Joomla not.

Both have SMF bridge modules available. For future reference, Drupal's is named "SMFforum Integration".

mmalmi@cc.hut.fi wrote:
> I don't have the time to configure it today, but I made a temporary
> account "" with password "" and full permissions to
> /var/www/bitcoin. You can access it via ssh or sftp at port 30000.

Email #104

Date: Sat, 21 Nov 2009 12:50:00 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

I've done a Joomla site for a customer, and I must say I like Drupal better, mostly for the admin interface which is easier to use and integrated into the main site.

Images aren't loading properly over https, I'll check it out when I can.

It's easier to just change the bitcoin.org DNS entry, forum.bitcoin.org is not necessary.

We could see if we can get a free SSL certificate somewhere, like http://www.startssl.com/?app=1, so the users wouldn't get a security warning from a self-signed certificate. However I don't know if they give certificates for anonymously registered domains.

> Thanks, that worked, I got File Manager installed with SSH. I also
> uploaded a few themes into Drupal. I haven't thoroughly gone through
> all the available themes yet.
>
> Looked around at CMSes, Drupal and Joomla are popular. Consensus is
> Joomla has a better selection of themes and is easier to learn, though
> Drupal may be more intuitive for programmers and customization. Joomla
> better for CMS, Drupal better for blogs. Drupal's URLs are search
> engine friendly, Joomla not.
>
> Both have SMF bridge modules available. For future reference, Drupal's
> is named "SMFforum Integration".
>
> mmalmi@cc.hut.fi wrote:
>> I don't have the time to configure it today, but I made a temporary
>> account "" with password "" and full permissions to
>> /var/www/bitcoin. You can access it via ssh or sftp at port 30000.

Email #105

Date: Sat, 21 Nov 2009 21:46:52 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

To: mmalmi@cc.hut.fi

I'll go ahead with setting up Drupal then.

I don't think we should make the site https by default. It's still very unusual for the public part of sites to be https, probably because it introduces potential technical complications, delays and greater server load. As a user I'm a little annoyed when it takes time to verify the identity of some no-name site I casually came across. For me it seems like https sites fail to load a lot more often.

The important thing is to have SSL available for those who need it. Those who need SSL I think know to try inserting an "s" after http and see if it works. SMF has code that changes all the links to https if the URL handed in is https.

We could add a note on the registration page that if you want SSL, you can change http to https at any time and approve the self-signed certificate, or a link that does it, and the TOR page can mention it too.

We can look into getting a certificate later when things have settled down. With Class 1, no changes are allowed for a year, which is a risk if we find issues with the current host and have to change IP.

mmalmi@cc.hut.fi wrote:
> I've done a Joomla site for a customer, and I must say I like Drupal
> better, mostly for the admin interface which is easier to use and
> integrated into the main site.
>
> Images aren't loading properly over https, I'll check it out when I can.
>
> It's easier to just change the bitcoin.org DNS entry, forum.bitcoin.org
> is not necessary.
>
> We could see if we can get a free SSL certificate somewhere, like
> http://www.startssl.com/?app=1, so the users wouldn't get a security
> warning from a self-signed certificate. However I don't know if they
> give certificates for anonymously registered domains.
>
>> Thanks, that worked, I got File Manager installed with SSH. I also
>> uploaded a few themes into Drupal. I haven't thoroughly gone through
>> all the available themes yet.
>>
>> Looked around at CMSes, Drupal and Joomla are popular. Consensus is
>> Joomla has a better selection of themes and is easier to learn, though
>> Drupal may be more intuitive for programmers and customization. Joomla
>> better for CMS, Drupal better for blogs. Drupal's URLs are search
>> engine friendly, Joomla not.
>>
>> Both have SMF bridge modules available. For future reference, Drupal's
>> is named "SMFforum Integration".
>>
>> mmalmi@cc.hut.fi wrote:
>>> I don't have the time to configure it today, but I made a temporary
>>> account "" with password "" and full permissions to
>>> /var/www/bitcoin. You can access it via ssh or sftp at port 30000.
>
>

>

Email #106

Date: Sun, 22 Nov 2009 19:47:56 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: SEO friendly site transition
To: Martti Malmi <mmalmi@cc.hut.fi>

We need to do a continuity transition with bitcoin.org so the search engines don't think this is a new site and reset the site start date and PR data. Google allows a certain number of properties like IP address or content of the site to change without deleting your site history. To play it safe, when the IP address changes, the content better stay the same and vice versa. Even though not much rank has accumulated yet, the original start date becomes extremely important if the site gets popular later.

Steps:
1) copy the current bitcoin.org index.html to the new server exactly as-is.
2) switch the bitcoin.org DNS entry.
3) keep working on the drupal site behind the scenes.
4) after google has had time to update its records, we can switch over to the drupal site.

The timing works out well because we can switch to the new forum now and release the drupal site later when we're ready.

I'll see if I can figure out how to temporarily move drupal aside to drupal.php or /drupal/ or something where we can still easily get in and work on it.

Email #107

Date: Sun, 22 Nov 2009 22:22:57 +0200
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: SEO friendly site transition

That's ok.

I'll be afk 23.-25.11.

> We need to do a continuity transition with bitcoin.org so the search
> engines don't think this is a new site and reset the site start date
> and PR data. Google allows a certain number of properties like IP
> address or content of the site to change without deleting your site
> history. To play it safe, when the IP address changes, the content
> better stay the same and vice versa. Even though not much rank has
> accumulated yet, the original start date becomes extremely important if
> the site gets popular later.
>
> Steps:
> 1) copy the current bitcoin.org index.html to the new server exactly as-is.
> 2) switch the bitcoin.org DNS entry.
> 3) keep working on the drupal site behind the scenes.
> 4) after google has had time to update its records, we can switch over
> to the drupal site.
>
> The timing works out well because we can switch to the new forum now
> and release the drupal site later when we're ready.
>
> I'll see if I can figure out how to temporarily move drupal aside to
> drupal.php or /drupal/ or something where we can still easily get in
> and work on it.

Email #108

Date: Mon, 23 Nov 2009 05:48:19 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Access permissions required to fix Drupal

To: Martti Malmi <mmalmi@cc.hut.fi>

Drupal's .htaccess file which uses mod_rewrite to allow clean URLs
without the ? parameter is not working because its changes are rejected
because Apache is not configured with "AllowOverride All". This is
needed to make Drupal coexist with the other site the way we want.

I need access to change these files to fix it:
  /etc/apache2/sites-available/default
  /etc/apache2/sites-available/default-ssl

/etc/apache2/httpd.conf

Here's the planned fix. If you do it yourself, please still give me
access to httpd.conf in case I need to change it again later.

In /etc/apache2/sites-available/default
change the 2nd instance of "AllowOverride None"
to "AllowOverride All"

and in /etc/apache2/sites-available/default-ssl
change the 2nd instance of "AllowOverride AuthConfig"
to "AllowOverride All"

replace
/etc/apache2/httpd.conf
with
/home/maintenance/httpd.conf

This probably requires Apache to be restarted after.
(apache2ctl graceful)

Email #109

Date: Mon, 23 Nov 2009 08:44:35 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Access permissions required to fix Drupal

Done. I granted you access to all the files.

> Drupal's .htaccess file which uses mod_rewrite to allow clean URLs
> without the ? parameter is not working because its changes are rejected
> because Apache is not configured with "AllowOverride All". This is
> needed to make Drupal coexist with the other site the way we want.
>
> I need access to change these files to fix it:
> /etc/apache2/sites-available/default
> /etc/apache2/sites-available/default-ssl
> /etc/apache2/httpd.conf
>
> Here's the planned fix. If you do it yourself, please still give me
> access to httpd.conf in case I need to change it again later.

>
> In /etc/apache2/sites-available/default
> change the 2nd instance of "AllowOverride None"
>   to "AllowOverride All"
>
> and in /etc/apache2/sites-available/default-ssl
> change the 2nd instance of "AllowOverride AuthConfig"
>   to "AllowOverride All"
>
> replace
> /etc/apache2/httpd.conf
> with
> /home/maintenance/httpd.conf
>
> This probably requires Apache to be restarted after.
> (apache2ctl graceful)

Email #110

Date: Thu, 26 Nov 2009 00:26:33 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: bitcoin.org DNS change went through

To: Martti Malmi <mmalmi@cc.hut.fi>

The bitcoin.org DNS change went through about 12 hours ago. I'll wait another 12 hours and then change the Forum tab on bitcoin.sourceforge.net to go to http://www.bitcoin.org/smf/

For future reference, the changes in SMF to update the base url were:
   server settings->Forum URL
   themes and layout->attempt to reset all themes
   there's a path in smileys and message icons

Email #111

Date: Thu, 26 Nov 2009 17:45:42 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Bitweaver menu editor broken

To: Martti Malmi <mmalmi@cc.hut.fi>

The Bitweaver menu editor is broken, I can't change the Forum link. The "create and edit menu items" page comes up blank for me:

http://bitcoin.sourceforge.net/nexus/menu_items.php?menu_id=2

You try it, I'm stumped.

The Forum link should be changed to:
http://www.bitcoin.org/smf/

Email #112

Date: Fri, 27 Nov 2009 02:46:50 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitweaver menu editor broken

Fixed. I changed it directly in the database.

> The Bitweaver menu editor is broken, I can't change the Forum link.
> The "create and edit menu items" page comes up blank for me:
>
> http://bitcoin.sourceforge.net/nexus/menu_items.php?menu_id=2
>
> You try it, I'm stumped.
>
> The Forum link should be changed to:
> http://www.bitcoin.org/smf/

Email #113

Date: Sun, 29 Nov 2009 09:53:10 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Cc: Liberty Standard <newlibertystandard@gmail.com>

Subject: Google Wave

I just watched the Google Wave introduction video at wave.google.com.
It's the Google's open source proposal for a replacement for the
decades old e-mail protocol, and it looked quite cool. A "wave" is a
communication and collaboration unit that can be read and edited by
multiple users in real time and easily shared to new users, unlike
e-mail threads. It combines the functionality of instant messaging,
wikis, conventional e-mail and social networking, and supports
integration with external applications.

If you want invites, you can give me the e-mail addresses where you
want them to. If you already have Wave addresses, please give me them
as well. It would be great to see how the system works in practice.

Email #114

Date: Mon, 30 Nov 2009 14:13:04 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Bitcoin.org

The current site layout looks nice and simple. The logo just should be
changed. If we want to go live quickly, we can just replace it with
the site title and make a better logo later.

If we need help with site administration or contacts to professional
web graphic artists, we can ask Dave. He does Drupal stuff for work.

Email #115

Date: Mon, 30 Nov 2009 14:36:51 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

It would be also great if you can get the Sourceforge logo from the SF
project admin and add it to the site footer.

> The current site layout looks nice and simple. The logo just should be
> changed. If we want to go live quickly, we can just replace it with the

> site title and make a better logo later.
>
> If we need help with site administration or contacts to professional
> web graphic artists, we can ask Dave. He does Drupal stuff for work.

Email #116

Date: Mon, 30 Nov 2009 16:07:13 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

I autogenerated the new logo at http://cooltext.com/, it's a good
quick solution. You can try a wide variety of different logo styles
there if you have the patience for the slow user interface.

> It would be also great if you can get the Sourceforge logo from the SF
> project admin and add it to the site footer.
>
>> The current site layout looks nice and simple. The logo just should be
>> changed. If we want to go live quickly, we can just replace it with the
>> site title and make a better logo later.
>>
>> If we need help with site administration or contacts to professional
>> web graphic artists, we can ask Dave. He does Drupal stuff for work.

Email #117

Date: Mon, 30 Nov 2009 20:34:20 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

To: mmalmi@cc.hut.fi

Thanks, I haven't settled on a theme yet. My first experiment was to
try something besides yet another blue site. Another line of thought is
that it should be like a bank website, stately, professional and

official looking to support confidence in financial matters.

The logo's a little too Disco/web-1990's. I still like your bitweaver one better, I recreated it with text as a placeholder for now. When the theme is more settled, I'll think about a matching logo.

Good idea about the Sourceforge tag, we can use all the graphics we can get.

I have more to do before we go live, and we need to give the search engines more time.

mmalmi@cc.hut.fi wrote:
> I autogenerated the new logo at http://cooltext.com/, it's a good quick
> solution. You can try a wide variety of different logo styles there if
> you have the patience for the slow user interface.
>
>> It would be also great if you can get the Sourceforge logo from the SF
>> project admin and add it to the site footer.
>>
>>> The current site layout looks nice and simple. The logo just should be
>>> changed. If we want to go live quickly, we can just replace it with the
>>> site title and make a better logo later.
>>>
>>> If we need help with site administration or contacts to professional
>>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>
>
>

Email #118

Date: Wed, 02 Dec 2009 16:26:42 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

The text logo looks quite good actually, except on Windows when the font antialiasing doesn't work. I turned it into a png.

I just made a 10,000bc transaction from one account to another, but it ended up sending 10,000.20bc. Any idea why that could be?

> Thanks, I haven't settled on a theme yet. My first experiment was to
> try something besides yet another blue site. Another line of thought
> is that it should be like a bank website, stately, professional and
> official looking to support confidence in financial matters.
>
> The logo's a little too Disco/web-1990's. I still like your bitweaver
> one better, I recreated it with text as a placeholder for now. When
> the theme is more settled, I'll think about a matching logo.
>
> Good idea about the Sourceforge tag, we can use all the graphics we can get.
>
> I have more to do before we go live, and we need to give the search
> engines more time.
>
> mmalmi@cc.hut.fi wrote:
>> I autogenerated the new logo at http://cooltext.com/, it's a good
>> quick solution. You can try a wide variety of different logo styles
>> there if you have the patience for the slow user interface.
>>
>>> It would be also great if you can get the Sourceforge logo from the SF
>>> project admin and add it to the site footer.
>>>
>>>> The current site layout looks nice and simple. The logo just should be
>>>> changed. If we want to go live quickly, we can just replace it with the
>>>> site title and make a better logo later.
>>>>
>>>> If we need help with site administration or contacts to professional
>>>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>>
>>
>>

Email #119

Date: Wed, 02 Dec 2009 17:47:48 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

To: mmalmi@cc.hut.fi

What Windows version/browser doesn't font anti-aliasing work on? IE 6 on XP anti-aliases, and versions below that have less than 1% market share.

There's a transaction fee of 0.01 per KB after the first 1KB for oversized transactions. The first 1KB is free, small transactions are typically 250 bytes. Doubleclick on the transaction. Think of it like postage by weight.

The solution is an extra dialog when sending, something like "This is an oversized transaction and requires a transaction fee of 0.20bc. Is this OK?" (is that text good enough or any improvements?) I have the code already, I'll put it in.

Then we wouldn't have to explain the 10,000.20bc transaction, but may still have to explain who the transaction fee goes to.

mmalmi@cc.hut.fi wrote:
> The text logo looks quite good actually, except on Windows when the font
> antialiasing doesn't work. I turned it into a png.
>
> I just made a 10,000bc transaction from one account to another, but it
> ended up sending 10,000.20bc. Any idea why that could be?
>
>> Thanks, I haven't settled on a theme yet. My first experiment was to
>> try something besides yet another blue site. Another line of thought
>> is that it should be like a bank website, stately, professional and
>> official looking to support confidence in financial matters.
>>
>> The logo's a little too Disco/web-1990's. I still like your bitweaver
>> one better, I recreated it with text as a placeholder for now. When
>> the theme is more settled, I'll think about a matching logo.
>>
>> Good idea about the Sourceforge tag, we can use all the graphics we
>> can get.
>>
>> I have more to do before we go live, and we need to give the search
>> engines more time.
>>
>> mmalmi@cc.hut.fi wrote:
>>> I autogenerated the new logo at http://cooltext.com/, it's a good
>>> quick solution. You can try a wide variety of different logo styles
>>> there if you have the patience for the slow user interface.
>>>

>>>> It would be also great if you can get the Sourceforge logo from the SF
>>>> project admin and add it to the site footer.
>>>>
>>>>> The current site layout looks nice and simple. The logo just should be
>>>>> changed. If we want to go live quickly, we can just replace it with
>>>>> the
>>>>> site title and make a better logo later.
>>>>>
>>>>> If we need help with site administration or contacts to professional
>>>>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>>>
>>>
>>>
>
>
>

Email #120

Date: Thu, 03 Dec 2009 09:46:50 +0200
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoin.org

> What Windows version/browser doesn't font anti-aliasing work on? IE 6
> on XP anti-aliases, and versions below that have less than 1% market
> share.

Firefox on XP doesn't, and IE also doesn't produce as good quality as
I have on Linux. Screenshots from browsershots.org attached.

> There's a transaction fee of 0.01 per KB after the first 1KB for
> oversized transactions. The first 1KB is free, small transactions are
> typically 250 bytes. Doubleclick on the transaction. Think of it like
> postage by weight.

Is there no transaction fee then, if you send the same amount in
multiple small packages?

> The solution is an extra dialog when sending, something like "This is
> an oversized transaction and requires a transaction fee of 0.20bc. Is
> this OK?" (is that text good enough or any improvements?) I have the

> code already, I'll put it in.

Sounds fine.

> Then we wouldn't have to explain the 10,000.20bc transaction, but may
> still have to explain who the transaction fee goes to.

Where should it go btw? Here it went to the receiver along with all
the other coins. Transaction screenshot attached.

> mmalmi@cc.hut.fi wrote:
>> The text logo looks quite good actually, except on Windows when the
>> font antialiasing doesn't work. I turned it into a png.
>>
>> I just made a 10,000bc transaction from one account to another, but
>> it ended up sending 10,000.20bc. Any idea why that could be?
>>
>>> Thanks, I haven't settled on a theme yet. My first experiment was to
>>> try something besides yet another blue site. Another line of thought
>>> is that it should be like a bank website, stately, professional and
>>> official looking to support confidence in financial matters.
>>>
>>> The logo's a little too Disco/web-1990's. I still like your bitweaver
>>> one better, I recreated it with text as a placeholder for now. When
>>> the theme is more settled, I'll think about a matching logo.
>>>
>>> Good idea about the Sourceforge tag, we can use all the graphics
>>> we can get.
>>>
>>> I have more to do before we go live, and we need to give the search
>>> engines more time.
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> I autogenerated the new logo at http://cooltext.com/, it's a good
>>>>   quick solution. You can try a wide variety of different logo
>>>> styles there if you have the patience for the slow user interface.
>>>>
>>>>> It would be also great if you can get the Sourceforge logo from the SF
>>>>> project admin and add it to the site footer.
>>>>>
>>>>>> The current site layout looks nice and simple. The logo just should be
>>>>>> changed. If we want to go live quickly, we can just replace it with the
>>>>>> site title and make a better logo later.

>>>>>>
>>>>>> If we need help with site administration or contacts to professional
>>>>>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>>>>
>>>>
>>>>
>>
>>
>>

Email #121

Date: Fri, 04 Dec 2009 04:24:41 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
>> What Windows version/browser doesn't font anti-aliasing work on? IE 6
>> on XP anti-aliases, and versions below that have less than 1% market
>> share.
>
> Firefox on XP doesn't, and IE also doesn't produce as good quality as I
> have on Linux. Screenshots from browsershots.org attached.

That's strange, I've seen Firefox 3.5 on XP anti-alias large fonts.
Well anyway, your way is safer.

I changed it back to text for now though so I can keep tweaking the
colours. Drupal puts the tags and junk in the browser title but
that's fine for testing.

I added some instruction text on the homepage below the screenshots.

> Is there no transaction fee then, if you send the same amount in
> multiple small packages?

True. I suppose the dialog could make it worse by giving people a
chance to experiment with breaking it up.

I'm making some changes. The largest free transaction will be 60KB, or about 27,000bc if made of 50bc inputs. I hope that's high enough that the transaction fee should rarely ever come up. v0.2 nodes will take free transactions until the block size is over 200K, with priority given to smaller transactions.

It's best if you don't talk about this transaction fee stuff in public. It's there for flood control. We don't want to give anyone any ideas.

> Where should it go btw? Here it went to the receiver along with all the
> other coins. Transaction screenshot attached.

You found an infrequent bug in CreateTransaction. It wrote the transaction for 10000.20 with a fee of 0.22. If you look at the transaction on the sender's side, it'll be a debit 10000.42 with transaction fee 0.22. The bug was that it had to make a rare third pass on calculating the fee, and incorrectly added the first pass' fee to the amount being sent. Will fix.

Email #122

Date: Sun, 06 Dec 2009 03:21:00 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Sourceforge tracker

To: mmalmi@cc.hut.fi

I added the sourceforge tracker to bitcoin.sourceforge.net. The complete selection of links is below if you want a different one.

I had it on bitcoin.org for a minute, but took it off. It breaks the lock in SSL mode with a mixed content warning, "partially encrypted" and "contains unauthenticated content". Anyway, do we really want sourceforge tracking everyone? It's more privacy friendly without it.

The available logos and the correct HTML to use for the Bitcoin project are:

Logo 1 (Dimensions: 80 x 15; Background: Black)

HTML Code: <img src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&type=8"

width="80" height="15" alt="Get Bitcoin at SourceForge.net. Fast, secure and Free Open Source software downloads" />

Logo 2 (Dimensions: 80 x 15; Background: Silver)

HTML Code:

Logo 3 (Dimensions: 80 x 15; Background: White)

HTML Code:

Logo 4 (Dimensions: 120 x 30; Background: Black)

HTML Code:

Logo 5 (Dimensions: 120 x 30; Background: Silver)

HTML Code:

Logo 6 (Dimensions: 120 x 30; Background: White)

HTML Code:

Logo 7 (Dimensions: 150 x 40; Background: Black)

HTML Code: <img src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&type=14" width="150" height="40" alt="Get Bitcoin at SourceForge.net. Fast,

secure and Free Open Source software downloads" />

Logo 8 (Dimensions: 150 x 40; Background: Silver)

HTML Code: <img
src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&type=15"
width="150" height="40" alt="Get Bitcoin at SourceForge.net. Fast,
secure and Free Open Source software downloads" />

Logo 9 (Dimensions: 150 x 40; Background: White)

HTML Code: <img
src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&type=16"
width="150" height="40" alt="Get Bitcoin at SourceForge.net. Fast,
secure and Free Open Source software downloads" />

mmalmi@cc.hut.fi wrote:
> It would be also great if you can get the Sourceforge logo from the SF
> project admin and add it to the site footer.
>
>> The current site layout looks nice and simple. The logo just should be
>> changed. If we want to go live quickly, we can just replace it with the
>> site title and make a better logo later.
>>
>> If we need help with site administration or contacts to professional
>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>
>
>

Email #123

Date: Mon, 07 Dec 2009 13:49:08 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Sourceforge tracker

I made a copy of the logo onto the local server, so we can still use
it for graphics. It's not disallowed by the SF trademark policy.

> I added the sourceforge tracker to bitcoin.sourceforge.net. The

> complete selection of links is below if you want a different one.
>
> I had it on bitcoin.org for a minute, but took it off. It breaks the
> lock in SSL mode with a mixed content warning, "partially encrypted"
> and "contains unauthenticated content". Anyway, do we really want
> sourceforge tracking everyone? It's more privacy friendly without it.
>
> mmalmi@cc.hut.fi wrote:
>> It would be also great if you can get the Sourceforge logo from the
>> SF project admin and add it to the site footer.
>>
>>> The current site layout looks nice and simple. The logo just should be
>>> changed. If we want to go live quickly, we can just replace it with the
>>> site title and make a better logo later.
>>>
>>> If we need help with site administration or contacts to professional
>>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>>
>>
>>

Email #124

Date: Tue, 08 Dec 2009 05:43:33 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Drupal site online

To: Martti Malmi <mmalmi@cc.hut.fi>

I went ahead and put the new Drupal site online. Enough time has passed for a safe transition, and the site looks good. There's more work I should do on the theme, but it's good enough so far. This is a huge improvement over the old bitcoin.org page.

Email #125

Date: Tue, 08 Dec 2009 12:50:20 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Drupal site online

Good job. I redirected bitcoin.sourceforge.net there.

> I went ahead and put the new Drupal site online. Enough time has
> passed for a safe transition, and the site looks good. There's more
> work I should do on the theme, but it's good enough so far. This is a
> huge improvement over the old bitcoin.org page.

Email #126

Date: Fri, 11 Dec 2009 03:30:10 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: custom3 theme

To: Martti Malmi <mmalmi@cc.hut.fi>

I wasn't satisfied with my custom2 theme. It felt crowded, the
header/logo seemed wrong and the heavy left margin stationery style is
outdated.

custom3 online now is a more standard layout similar to a lot of
commercial software homepages. Maybe it's just me, but I really like
the random blue squares.

Email #127

Date: Sun, 13 Dec 2009 22:12:38 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Version 0.2 almost ready to release

> It's almost time to release version 0.2. If you have a minute, could
> you try this release candidate (attached)? If there aren't any
> problems and I don't think of anything I missed, this could be released
> in a day or two.

No problems so far. Seems fine.

> I zipped the setup exe because I doubt the e-mail servers will allow
> exe attachments. I'm not sure it'll allow zip either, but pretty sure
> the tar.gz one will get through.
>
> Attachments:
> 3,092,916 bitcoin-0.2.0-setup.zip
> 2,402,522 bitcoin-0.2.0-linux.tar.gz
> 3,061,059 bitcoin-0.2.0-win32.zip

Both got through here.

Email #128

Date: Tue, 15 Dec 2009 06:40:04 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: RC2

> Found something I felt I had to fix with the initial block download.
> Do you mind testing an initial block download again?

The first time I tried it on Windows, the initial download took a few minutes to start, even though it got many connections quickly. I tried again twice, and didn't have the same problem again. I don't know whether it's related to your latest update or not.

On Ubuntu it worked fine.

> Hope this isn't in the middle of your final exams right now.

Well actually it is, but it's not too bad. Time is a matter of arrangement.

Email #129

Date: Wed, 16 Dec 2009 04:57:36 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: RC2

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> The first time I tried it on Windows, the initial download took a few
> minutes to start, even though it got many connections quickly. I tried
> again twice, and didn't have the same problem again. I don't know
> whether it's related to your latest update or not.

Most of the fixes are on the sender's side, so if you were downloading the network upgrades to 0.2.

How long did the initial download take?

Email #130

Date: Wed, 16 Dec 2009 17:41:41 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: RC2

>> The first time I tried it on Windows, the initial download took a
>> few minutes to start, even though it got many connections quickly.
>> I tried again twice, and didn't have the same problem again. I
>> don't know whether it's related to your latest update or not.
>
> Most of the fixes are on the sender's side, so if you were downloading
> from a 0.1.5 node, some problems are still there. It'll get better as
> the network upgrades to 0.2.
>
> How long did the initial download take?

About 1,5h.

Email #131

Date: Wed, 16 Dec 2009 16:54:46 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Planned release announcement text

To: Martti Malmi <mmalmi@cc.hut.fi>

Here's the planned release announcement text. Probably releasing shortly.

Bitcoin version 0.2 is here!

Download links:
Windows Setup Program
Windows Zip File
Linux (tested on Ubuntu)

New features

Martti Malmi
- Minimize to system tray option
- Autostart on boot option so you can keep it running in the background automatically
- New options dialog layout for future expansion
- Setup program for Windows
- Linux version

Satoshi Nakamoto
- Multi-processor support for coin generation
- Proxy support for use with TOR
- Fixed some slowdowns in the initial block download
- Various refinements to keep the network running smoothly

We also have a new forum at http://www.bitcoin.org/smf/ if you have any questions.

Thanks to Martti Malmi (sirius-m) for his coding work and for hosting the new site and forum, and thanks to New Liberty Standard for testing the Linux version.

Satoshi Nakamoto

Email #132

Date: Thu, 17 Dec 2009 06:49:02 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: [bitcoin-list] Bitcoin 0.2 released
To: bitcoin-list@lists.sourceforge.net

Bitcoin 0.2 is here!

Download (Windows, and now Linux version available)
http://sourceforge.net/projects/bitcoin/files/

New Features

Martti Malmi
  - Minimize to system tray option
  - Autostart on boot option so you can keep it running in the
background automatically
  - New options dialog layout for future expansion
  - Setup program for Windows
  - Linux version (tested on Ubuntu)
Satoshi Nakamoto
  - Multi-processor support for coin generation
  - Proxy support for use with TOR
  - Fixed some slowdowns in the initial block download

We also have a new forum at http://www.bitcoin.org/smf/

Many thanks to Martti (sirius-m) for all his development work, and to
New Liberty Standard for his help with testing the Linux version.

Satoshi Nakamoto

Email #133

Date: Tue, 22 Dec 2009 15:49:14 +0200

From: mmalmi@cc.hut.fi

To: satoshin@gmx.com

Subject: Bitcoin stuff

I have registered the domain name bitcoinexchange.com and will start
coding the service sometime soon as a nice leisure activity. I'm
envisioning a simple Google-like interface with no registration and
only two texts fields on the front page, where you insert the amount

of money you wish to trade, and either your PayPal address to buy dollars or bitcoin address to buy bitcoins. On the next page you'll get a new bitcoin address for sending the coins or a check code for the PayPal transaction text.

PayPal is good for the beginning - it's simple and has no startup costs, but later on I might accept credit cards also.

Do you still need the maintenance account? It's ok if you do, but change the password to something else.

Email #134

Date: Tue, 22 Dec 2009 19:00:41 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin stuff

To: mmalmi@cc.hut.fi

Thanks for creating the maintenance account, it would have been impossible to do all that without it. I'm really always going to need it. OK, I changed the password to a 20 character random password.

That's a good domain. People rarely type domain names anymore, they use autocomplete or click links on search engines.

I need to make a way for you to programmatically get new generated bitcoin addresses. Either that or you could have them send to your IP address, but then you have to rely on them to put the order number in the comment.

When generating the new address, there can be an option to add an entry to the address book associated with the address, so the received transaction will be labelled. I kinda hid the labels after early users found them confusing, but it would be very helpful for this application. You have to widen up the comment column to see them.

Are you going to manually review and enter orders, at least to begin with? I sure would.

I'm thinking I should move the UI in the direction of having the user ask for their bitcoin address when they want one. "give me a bitcoin to receive a payment with". I suppose next to the send button, there would

by a receive button, you press it and it says "here's a new address to use, here's the button to copy it to the clipboard, do you want to label it?" and maybe some explanation about why you shouldn't reuse addresses.

Or maybe just a "New Address" button next to the address box that you should hit each time to change it.

mmalmi@cc.hut.fi wrote:
> I have registered the domain name bitcoinexchange.com and will start
> coding the service sometime soon as a nice leisure activity. I'm
> envisioning a simple Google-like interface with no registration and only
> two texts fields on the front page, where you insert the amount of money
> you wish to trade, and either your PayPal address to buy dollars or
> bitcoin address to buy bitcoins. On the next page you'll get a new
> bitcoin address for sending the coins or a check code for the PayPal
> transaction text.
>
> PayPal is good for the beginning - it's simple and has no startup costs,
> but later on I might accept credit cards also.
>
> Do you still need the maintenance account? It's ok if you do, but change
> the password to something else.
>

Email #135

Date: Wed, 23 Dec 2009 11:12:03 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin stuff

> I need to make a way for you to programmatically get new generated
> bitcoin addresses. Either that or you could have them send to your IP
> address, but then you have to rely on them to put the order number in
> the comment.

I'd also need at least the command line tools to check if coins have been received and to send coins. It would require some way to communicate with the Bitcoin process running in the background. I don't know how that should be done, maybe with something RPC related.

It would also be great if the background process was non-graphical -

the VPS on the current service level doesn't have enough memory to run the X Windowing environment, unless I come up with some ways to free memory.

> Are you going to manually review and enter orders, at least to begin
> with? I sure would.

Yes, at least to begin with, when the customer sells bc's and receives dollars. I wouldn't give a script the access to my dollar reserves so lightly. The other way around (customer's dollars -> bitcoins) it doesn't feel that insecure, and it's certainly nicer for the customer to receive his bitcoins immediately.

> mmalmi@cc.hut.fi wrote:
>> I have registered the domain name bitcoinexchange.com and will
>> start coding the service sometime soon as a nice leisure activity.
>> I'm envisioning a simple Google-like interface with no registration
>> and only two texts fields on the front page, where you insert the
>> amount of money you wish to trade, and either your PayPal address
>> to buy dollars or bitcoin address to buy bitcoins. On the next page
>> you'll get a new bitcoin address for sending the coins or a check
>> code for the PayPal transaction text.
>>
>> PayPal is good for the beginning - it's simple and has no startup
>> costs, but later on I might accept credit cards also.
>>
>> Do you still need the maintenance account? It's ok if you do, but
>> change the password to something else.
>>

Email #136

Date: Wed, 23 Dec 2009 17:53:18 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin stuff

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> I'd also need at least the command line tools to check if coins have
> been received and to send coins. It would require some way to

> communicate with the Bitcoin process running in the background. I don't
> know how that should be done, maybe with something RPC related.
>
> It would also be great if the background process was non-graphical - the
> VPS on the current service level doesn't have enough memory to run the X
> Windowing environment, unless I come up with some ways to free memory.

I had been wondering why everyone keeps harping on no-UI, when already you can run it with only a small icon on the tray, which is common for server services on Windows. So I guess this is why. I had chalked it up to unix snobbery if they couldn't abide a tiny little icon on a desktop they never see.

Not opening any windows is easy, but it may fail because the gtk libraries aren't there. wxWidgets has __WXBASE__ for "Only wxBase, no GUI features". You could try building for that instead of __WXGTK__ and see what happens. It would be preferable if there's any way to do it as a command line switch on the same executable, rather than yet another build variation to release.

How much memory do you have to work with? Bitcoin necessarily takes a fair bit of memory; about 75MB on Windows. Is that a problem?

Command line control is one of the next things on the list. I want to design the API carefully.

Receiving payments is the part that has a lot of design choices to be made. The caller needs to identify the transactions of interest, that's where the one-bitcoin-address-per-transaction model helps. Searching the comments text for an order number is another possibility. There's polled, asking what has been received to the given bitcoin address, and event driven. I guess in event driven, bitcoin would be told to run a command line when a certain amount is received to a certain bitcoin address.

Email #137

Date: Fri, 25 Dec 2009 15:25:43 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin stuff

> How much memory do you have to work with?
The VPS has 320MB RAM, 50MB of which is currently free. There's also
500MB swap space.

> Bitcoin necessarily takes a
> fair bit of memory; about 75MB on Windows. Is that a problem?

Sure about that? Windows task manager shows about 13MB memory usage here.

Email #138

Date: Fri, 25 Dec 2009 16:11:14 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoin stuff
To: mmalmi@cc.hut.fi

You're right, I was looking at a test run with 250,000 blocks... duh.

A normal one shows 17MB memory usage and 10MB VM size.

mmalmi@cc.hut.fi wrote:
>> How much memory do you have to work with?
> The VPS has 320MB RAM, 50MB of which is currently free. There's also
> 500MB swap space.
>
>> Bitcoin necessarily takes a
>> fair bit of memory; about 75MB on Windows. Is that a problem?
>
> Sure about that? Windows task manager shows about 13MB memory usage here.
>

Email #139

Date: Tue, 05 Jan 2010 03:55:14 +0200
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Bitcoin Exchange

I have a prototype of the bitcoinexchange.com service up now (auth: bitcoin/bit). It's running on the Python-powered Django web application framework, which is a pleasure to work with, compared to php.

I'll have to do some studying for a few days now, after which I can return to work with the exchange service. Among other things I'll fix the pricing so that the price of Bitcoins grows towards infinity when my supply of them gets closer to zero. That way I can find the market rate and stay at the point where supply meets demand. I'm not yet completely sure what the parameters of the hyperbolic pricing curve should be, so that's something to think about.

Email #140

Date: Wed, 03 Feb 2010 11:27:17 +0200

From: mmalmi@cc.hut.fi

To: satoshin@gmx.com

Subject: Bitcoin API

Have you decided upon the inter-process calling method of the Bitcoin API yet? An easy solution would be the socket interface provided by wxWidgets: http://docs.wxwidgets.org/trunk/overview_ipc.html. The Bitcoin program running a wxServer could be then accessed by calling the bitcoin executable from the command line or by coding your own wxClient app.

Another option would be to just use the plain BSD sockets.

Can you send me a 64-bit Linux binary of Bitcoin if you have one? I tried compiling on the VPS, but it ran out of memory. Tried the 32-bit version (with ia32-libs) also, but it didn't find the shared libraries.

Email #141

Date: Thu, 04 Feb 2010 02:20:10 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Exchange ideas

To: Martti Malmi <mmalmi@cc.hut.fi>

You could always exchange for Liberty Reserve. It's an online currency similar to e-Bullion, Pecunix or Webmoney that allows exchanges no questions asked and with privacy.

LR and the others are hard to buy but easy to cash out. Hard to buy because exchangers are very cautious about getting ripped off by reversed payments, so they require more details and holding time. Cashing out is very easy. LR is non-reversible, so there are oodles of exchanges eager to turn LR into any kind of payment.

Bitcoin is the reverse, in that it's easy to get Bitcoins just by generating them. It would be easy for customers to go bitcoin->LR->cash, bitcoin->LR->gold, bitcoin->LR->paypal or maybe they just want to save the money, then just bitcoin->LR.

There's also the idea BTC2PSC had to sell paysafecards for bitcoins. Either online delivery by sending the card number by e-mail, or delivery of the unopened physical card in the mails. There are many variations of these cards. In some countries, they're called Gift Cards, and can be used wherever credit cards are accepted. I think they're used more by people who don't have the credit history to get a real credit card, so they buy gift cards themselves to pay for things that require a credit card.

Email #142

Date: Thu, 04 Feb 2010 01:32:50 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Exchange options

To: Martti Malmi <mmalmi@cc.hut.fi>

Don't rush ahead and get yourself rejected from all the payment options before you've had time to see if there's a better approach. I suggest you wait before contacting any more payment processors. You may get ideas from things other users come up with and try.

Just some random incomplete ideas: There may be a way to position it as an intermediate credit for micropayments for some virtual good or something. Or maybe if the payments are only in one direction. If you only buy bitcoins, then you're only sending money out not taking people's money, that would still be useful to peg the currency. That

might be payment for computer time.

Credit card is only one way. Don't even talk about the idea of returning money to customer's credit cards. Credit card companies hate that.

In any case, any payment processor is going to expect you to be selling something real.

Do you have electronic transfer or paper cheque in your country? (even if only within Europe)

Email #143

Date: Wed, 03 Feb 2010 20:25:53 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin API

To: mmalmi@cc.hut.fi

Is there any way to find out what the missing shared libraries are? It would help to know.

It probably needs the gtk libraries, in which case you'll have the same problem with the 64-bit version. I would like to have a single executable that can also run on a UI-less system, but I'm not sure how on linux to link to things but still be able to run and not use them if the library is not present. Maybe we should statically link the GTK. Licensewise, it's LGPL, but since it's only used on unix, that would be OK. (we can't link LGPL stuff on windows because we provide the OpenSSL DLL, but on linux OpenSSL comes with the OS)

My 64-bit (debug stripped) executable is attached. It includes untested changes that are not in SVN yet: UI changes and the wallet fSpent flag resync stuff.

I've been researching options for interprocess calling. I want something that will be easy for a variety of server side languages to call, particularly PHP. Cross-platform to windows is a plus.

I'm not sure if I want it to be something that can be accessed across the network. That would introduce security issues. If it can only be accessed on the local system, then local security authentication covers it, and it is incapable of being hacked remotely.

At surface level, not looking into any details yet, the current front runners are:
D-Bus:
    local system only
    used by qt, gnome and skype
    bindings: c, python, java, c++,
          php listed as "in progress"
          .net listed as unmaintained
          not sure how ready it is on windows
XML-RPC:
    widely used, built in libraries on PHP
    it's more for web clients to talk to server, transport is http, so its a security question

Is it possible to open a socket that can only be accessed locally?

mmalmi@cc.hut.fi wrote:
> Have you decided upon the inter-process calling method of the Bitcoin
> API yet? An easy solution would be the socket interface provided by
> wxWidgets: http://docs.wxwidgets.org/trunk/overview_ipc.html. The
> Bitcoin program running a wxServer could be then accessed by calling the
> bitcoin executable from the command line or by coding your own wxClient
> app.
>
> Another option would be to just use the plain BSD sockets.
>
> Can you send me a 64-bit Linux binary of Bitcoin if you have one? I
> tried compiling on the VPS, but it ran out of memory. Tried the 32-bit
> version (with ia32-libs) also, but it didn't find the shared libraries.
>

Email #144

Date: Thu, 04 Feb 2010 19:47:36 +0200
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoin API

> Is there any way to find out what the missing shared libraries are? It
> would help to know.

> This is what "ldd bitcoin" says:
>
> ```
>         linux-gate.so.1 =>  (0xf778c000)
>         libcrypto.so.0.9.8 => /usr/lib32/i686/cmov/libcrypto.so.0.9.8
> (0xf762a000)
>         libgtk-x11-2.0.so.0 => not found
>         libgthread-2.0.so.0 => not found
>         libSM.so.6 => /usr/lib32/libSM.so.6 (0xf7621000)
>         libstdc++.so.6 => /usr/lib32/libstdc++.so.6 (0xf7533000)
>         libm.so.6 => /lib32/libm.so.6 (0xf750f000)
>         libgcc_s.so.1 => /usr/lib32/libgcc_s.so.1 (0xf7502000)
>         libc.so.6 => /lib32/libc.so.6 (0xf73b0000)
>         libdl.so.2 => /lib32/libdl.so.2 (0xf73ac000)
>         libgdk-x11-2.0.so.0 => not found
>         libXinerama.so.1 => /usr/lib32/libXinerama.so.1 (0xf73a8000)
>         libgdk_pixbuf-2.0.so.0 => not found
>         libX11.so.6 => /usr/lib32/libX11.so.6 (0xf72b9000)
>         libpango-1.0.so.0 => not found
>         libgobject-2.0.so.0 => not found
>         libglib-2.0.so.0 => not found
>         libpthread.so.0 => /lib32/libpthread.so.0 (0xf72a1000)
>         libpng12.so.0 => /usr/lib32/libpng12.so.0 (0xf727e000)
>         libz.so.1 => /usr/lib32/libz.so.1 (0xf7269000)
>         libICE.so.6 => /usr/lib32/libICE.so.6 (0xf7251000)
>         /lib/ld-linux.so.2 (0xf778d000)
>         libXext.so.6 => /usr/lib32/libXext.so.6 (0xf7243000)
>         libxcb-xlib.so.0 => /usr/lib32/libxcb-xlib.so.0 (0xf7241000)
>         libxcb.so.1 => /usr/lib32/libxcb.so.1 (0xf7229000)
>         libXau.so.6 => /usr/lib32/libXau.so.6 (0xf7226000)
>         libXdmcp.so.6 => /usr/lib32/libXdmcp.so.6 (0xf7220000)
> ```
>
> Notfounds seem to be gtk-libraries indeed. I have those files in my
> /usr/lib folder, but maybe they're ignored because they're 64bit, or
> maybe only /usr/lib32 is searched. I haven't tested on other 64bit
> machines.
>
> > My 64-bit (debug stripped) executable is attached. It includes
> > untested changes that are not in SVN yet: UI changes and the wallet
> > fSpent flag resync stuff.
>
> The package doesn't open, it says "not in gzip format".
>
> > Is it possible to open a socket that can only be accessed locally?

Yes, you can use IPC sockets ("Unix domain sockets") which are local only. That's done in the wx-api by using a filename in place of a port number. I committed an example of how the wxServer-Client communication is used, you can revert if you want to. Now there's the -blockamount command line option which asks the running instance for the block chain length.

I think this command line method could already be used from PHP, but it might be lighter if php itself could call the socket server directly. The wx's IPC overview mentions wxSocketEvent, wxSocketBase, wxSocketClient and wxSocketServer as being "Classes for the low-level TCP/IP API", which might be easier to use from php than what I used now (wxServer, wxClient, wxConnection). I'll look more into it.

Email #145

Date: Thu, 04 Feb 2010 18:50:35 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoin API
To: mmalmi@cc.hut.fi

I must have accidentally typed j instead of z. It's bz2 format. Rename to .tar.bz2 or just do tar -jxvf

> The package doesn't open, it says "not in gzip format".
>

Email #146

Date: Thu, 04 Feb 2010 19:33:26 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: UTF-8 to ANSI hack in CAboutDialog
To: Martti Malmi <mmalmi@cc.hut.fi>

What was the reason for this change?

#if !wxUSE_UNICODE
...

```
     if (str.Find('Â') != wxNOT_FOUND)
         str.Remove(str.Find('Â'), 1);
to:
     if (str.Find('ï¿½') != wxNOT_FOUND)
         str.Remove(str.Find('ï¿½'), 1);
```

wxFormBuilder turns the (c) symbol into UTF-8 automatically. On wxWidgets-2.8.9 ansi, it shows as a copyright symbol with an extra trash character, which this hack fixes up for the non-unicode (ansi) case.

Email #147

Date: Thu, 04 Feb 2010 19:59:48 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin API

To: mmalmi@cc.hut.fi

Good, then no need to consider d-bus. Is there something like IPC sockets on Windows? I guess we could look how wx does it, or maybe the XML-RPC library will already know what to do. Windows has named pipes, maybe that's the best analogue.

I don't think I want to invent my own RPC protocol, I want to use an existing standard. PHP, Java, Python or anything will be able to talk to the server directly the same way the command line commands do.

I'm going to start reading on XML-RPC. It's coming up in searches as the most widely used protocol and widely supported. PHP includes it in its standard libraries.

>> Is it possible to open a socket that can only be accessed locally?
>
> Yes, you can use IPC sockets ("Unix domain sockets") which are local
> only. That's done in the wx-api by using a filename in place of a port
> number. I committed an example of how the wxServer-Client communication
> is used, you can revert if you want to. Now there's the -blockamount
> command line option which asks the running instance for the block chain
> length.
>
> I think this command line method could already be used from PHP, but it
> might be lighter if php itself could call the socket server directly.
> The wx's IPC overview mentions wxSocketEvent, wxSocketBase,

> wxSocketClient and wxSocketServer as being "Classes for the low-level
> TCP/IP API", which might be easier to use from php than what I used now
> (wxServer, wxClient, wxConnection). I'll look more into it.
>
>
>

Email #148

Date: Fri, 05 Feb 2010 04:08:54 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin API research status

To: Martti Malmi <mmalmi@cc.hut.fi>

I noticed this in the docs for wxSocketServer::Accept(bool wait = true):
"If wait is true and there are no pending connections to be accepted, it
will wait for the next incoming connection to arrive. **Warning: This
will block the GUI."

wxWidgets is pathologically single-threaded. Not only single-threaded,
but must-be-the-GUI-thread-ed. Even for something as non-UI as
wxStandardPaths I got nailed. All this is fine for UI code, since this
is the same constraint placed by Windows anyway, but for UI-less server
daemon code, wx calls are uncertain.

Status of my research currently:

For PHP, Python, etc to access the server, we need to use regular
sockets. I think we can make it local-only by binding to localhost
only, so it can only be accessed through the loopback. They say it's
also watertight to simply check the IP of connections received and
disconnect anything not 127.0.0.1. May as well do both.

XML-RPC is a bit fat. There are 4 libraries for C++ but they're all big
and hard to build, dependencies, license issues. Some posters complain
all the C++ and PHP XML-RPC libraries are buggy.

JSON-RPC is a simpler more elegant standard. It's simple enough I could
use a generic JSON parser.

PHP, Python and Java all have good implementations of JSON-RPC.

I'm currently leaning towards JSON-RPC.

Email #149

Date: Fri, 05 Feb 2010 09:16:23 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: UTF-8 to ANSI hack in CAboutDialog

I didn't change it knowingly, must have been some encoding problem.

> What was the reason for this change?
>
> #if !wxUSE_UNICODE
> ...
>   if (str.Find('Â') != wxNOT_FOUND)
>   str.Remove(str.Find('Â'), 1);
> to:
>   if (str.Find('ï¿½') != wxNOT_FOUND)
>   str.Remove(str.Find('ï¿½'), 1);
>
> wxFormBuilder turns the (c) symbol into UTF-8 automatically. On
> wxWidgets-2.8.9 ansi, it shows as a copyright symbol with an extra
> trash character, which this hack fixes up for the non-unicode (ansi)
> case.

Email #150

Date: Fri, 05 Feb 2010 09:56:16 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Exchange options

Liberty Reserve sounds good. I could first make a service that only accepts LR, and add more options later. The weakness is that buying LR is an extra step of inconvenience when the customer just wants to get Bitcoins. But maybe I don't have too much choice here.

> Do you have electronic transfer or paper cheque in your country? (even
> if only within Europe)

Yes, electronic bank transfer is available. During 2010 most European countries will become a part of SEPA (Single Euro Payments Area), which means that all payments within Europe are to be considered domestic. Banks will have to apply the same fees and standards to all domestic transfers, so they'll probably all be free of charge and complete in one bank day. For international transfers there's the SWIFT/IBAN system, which usually costs some extra.

A longer term project for my exchange service would be to see what kinds of integration options the banks have to offer. Bank transfers would reach nearly as many customers as credit cards do.

Email #151

Date: Fri, 05 Feb 2010 18:29:12 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Exchange options

To: mmalmi@cc.hut.fi

Maybe the current difficulty of buying LR is already the limit of how easy it can get in that direction.

Every conventional payment method has refutability as their way to cope with their lack of passwords and crypto. The system is wide open to copying plaintext credit card numbers and account numbers, and they deal with it by reversing the transaction after the fact. The system works for physical goods that have to be delivered somewhere, and services which can't be resold. It's a problem when it interfaces with precious metals and currency conversion.

The first step of being easy in one direction, bitcoin->LR or anything of established value, goes a long way. Even those who don't use the conversion still benefit from knowing that they could. Trading bitcoin becomes an easier way to trade the ability to claim LR, similar to how paper money was once the right to claim gold. Nobody has to ever actually claim the LR to get the benefit of having the option that they could if they wanted to.

A lot of times you just need a minuscule amount of online currency. The

hassle of buying the other online currencies is too much for buying a small amount. The ease of getting a small amount of bitcoin may help bootstrap an ecosystem of sellers of micropayment sized online goods selling to that market. If the sellers can get LR for bitcoins, they're happy, and that may be subsidized at first by investors who want to buy bc in large lots.

The main thing holding online currencies back is the lack of an easy way to get a small amount of currency. Bitcoin opens that up. It'll be the only online currency that's both easy to cash out and easy to get a small amount. It'll just be the usual harder difficulty to buy a large amount.

mmalmi@cc.hut.fi wrote:
> Liberty Reserve sounds good. I could first make a service that only
> accepts LR, and add more options later. The weakness is that buying LR
> is an extra step of inconvenience when the customer just wants to get
> Bitcoins. But maybe I don't have too much choice here.
>
>> Do you have electronic transfer or paper cheque in your country? (even
>> if only within Europe)
>
> Yes, electronic bank transfer is available. During 2010 most European
> countries will become a part of SEPA (Single Euro Payments Area), which
> means that all payments within Europe are to be considered domestic.
> Banks will have to apply the same fees and standards to all domestic
> transfers, so they'll probably all be free of charge and complete in one
> bank day. For international transfers there's the SWIFT/IBAN system,
> which usually costs some extra.
>
> A longer term project for my exchange service would be to see what kinds
> of integration options the banks have to offer. Bank transfers would
> reach nearly as many customers as credit cards do.
>

Email #152

Date: Fri, 05 Feb 2010 18:39:18 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: UTF-8 to ANSI hack in CAboutDialog

To: mmalmi@cc.hut.fi

Right, I'll change it to this so it doesn't get broken again:

```
     if (str.Find('\xC2') != wxNOT_FOUND)
         str.Remove(str.Find('\xC2'), 1);
```

mmalmi@cc.hut.fi wrote:

> I didn't change it knowingly, must have been some encoding problem.
>
>> What was the reason for this change?
>>
>> #if !wxUSE_UNICODE
>> ...
>>   if (str.Find('Â') != wxNOT_FOUND)
>>   str.Remove(str.Find('Â'), 1);
>> to:
>>   if (str.Find('ï¿½') != wxNOT_FOUND)
>>   str.Remove(str.Find('ï¿½'), 1);
>>
>> wxFormBuilder turns the (c) symbol into UTF-8 automatically. On
>> wxWidgets-2.8.9 ansi, it shows as a copyright symbol with an extra
>> trash character, which this hack fixes up for the non-unicode (ansi)
>> case.
>
>
>

Email #153

Date: Sun, 07 Feb 2010 06:12:04 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: JSON-RPC status

To: Martti Malmi <mmalmi@cc.hut.fi>

The JSON-RPC implementation is going well. I'm using boost::asio for sockets. JSON-RPC can be plain socket or HTTP, but it seems most other implementations are HTTP, so I made my own simple HTTP headers. For JSON parsing I'm using JSON Spirit, which makes full use of STL and has been really nice to use. It's header-only so it's no added build work, and small enough to just add it to our source tree. MIT license. This should all be working in a few more days.

The forum sure is taking off. I didn't expect to have so much activity so fast.

Email #154

Date: Sun, 07 Feb 2010 12:45:53 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

That's great! I'll start familiarizing myself with Liberty Reserve and its api.

> The JSON-RPC implementation is going well. I'm using boost::asio for
> sockets. JSON-RPC can be plain socket or HTTP, but it seems most other
> implementations are HTTP, so I made my own simple HTTP headers. For
> JSON parsing I'm using JSON Spirit, which makes full use of STL and has
> been really nice to use. It's header-only so it's no added build work,
> and small enough to just add it to our source tree. MIT license. This
> should all be working in a few more days.
>
> The forum sure is taking off. I didn't expect to have so much activity
> so fast.

Email #155

Date: Mon, 08 Feb 2010 15:28:52 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Translation

To: Martti Malmi <mmalmi@cc.hut.fi>

Does Drupal have any special multi-language support, or do you just create copies of pages by hand?

BlueSky offered to do translation on the forum. If you create a www.bitcoin.org/zh/ copy of the site and give him an account with just the ability to create new pages and edit text, he'll probably translate the site into Chinese for you and maybe maintain it.

Email #156

Date: Tue, 09 Feb 2010 17:42:06 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Translation

Drupal supports multiple languages. I didn't yet figure out how to make it automatically show the translation at bitcoin.org/zh-hans though.

> Does Drupal have any special multi-language support, or do you just
> create copies of pages by hand?
>
> BlueSky offered to do translation on the forum. If you create a
> www.bitcoin.org/zh/ copy of the site and give him an account with just
> the ability to create new pages and edit text, he'll probably translate
> the site into Chinese for you and maybe maintain it.

Email #157

Date: Thu, 11 Feb 2010 20:50:12 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Translation

I got the translations working correctly, now it should automatically detect the language from the browser settings. Choosing manually is of course also possible. I asked the translators to send me their translations as pm or e-mail. I guess I'll make a Finnish translation myself at some point. Multiple translations add to the site's credibility.

Drupal is asking to do a security update. Do we have other customized files we need to backup than those located in the "sites" directory?

Email #158

Date: Thu, 11 Feb 2010 22:58:29 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Translation

To: mmalmi@cc.hut.fi

I didn't make any changes to Drupal code. The only thing other than installing themes was the .htaccess file (which really is needed, it didn't work in the global config file).

It was only SMF where I made some PHP changes.

You might find it preferable not to translate it into your own language. Often the standard answer about legalities is that it's only intended for people in other countries. Translating it into your home language weakens that argument.

mmalmi@cc.hut.fi wrote:
> I got the translations working correctly, now it should automatically
> detect the language from the browser settings. Choosing manually is of
> course also possible. I asked the translators to send me their
> translations as pm or e-mail. I guess I'll make a Finnish translation
> myself at some point. Multiple translations add to the site's credibility.
>
> Drupal is asking to do a security update. Do we have other customized
> files we need to backup than those located in the "sites" directory?
>

Email #159

Date: Fri, 12 Feb 2010 12:06:43 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Translation

I'm not too worried about that, since I'm not doing anything illegal, even with my exchange service. If I were, it wouldn't help me that I'm only offering the service for foreigners. Things may of course be different under other jurisdictions, but that's how it is in my country. The law monopoly here is less uncivilized than many others.

> You might find it preferable not to translate it into your own

> language. Often the standard answer about legalities is that it's only
> intended for people in other countries. Translating it into your home
> language weakens that argument.

Email #160

Date: Sat, 13 Feb 2010 01:08:42 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

To: mmalmi@cc.hut.fi

I uploaded my JSON-RPC and command line implementation to SVN. I'm
waiting to post on the forum when I've had more time to think about the
commands. At least some method names are going to change.

To enable the RPC server, add the switch -server. It's not on by default.

Client commands are without any switches, as such:
```
bitcoin getblockcount
bitcoin getdifficulty
bitcoin getnewaddress somelabel
bitcoin sendtoaddress 1DvqsbZ... 1.00
bitcoin getallpayments 0
bitcoin stop
```

Applications would normally use JSON-RPC directly, not command line.

I haven't tested my JSON-RPC server with anything else yet. If you do,
please tell me how it goes. You're using Python, right?

Getting the Linux version to run without the GTK installed will be a
separate task.

mmalmi@cc.hut.fi wrote:
> That's great! I'll start familiarizing myself with Liberty Reserve and
> its api.
>
>> The JSON-RPC implementation is going well. I'm using boost::asio for
>> sockets. JSON-RPC can be plain socket or HTTP, but it seems most other
>> implementations are HTTP, so I made my own simple HTTP headers. For
>> JSON parsing I'm using JSON Spirit, which makes full use of STL and has
>> been really nice to use. It's header-only so it's no added build work,

>> and small enough to just add it to our source tree. MIT license. This
>> should all be working in a few more days.
>>
>> The forum sure is taking off. I didn't expect to have so much activity
>> so fast.
>
>
>

Email #161

Date: Sun, 14 Feb 2010 19:55:51 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

> I haven't tested my JSON-RPC server with anything else yet. If you do,
> please tell me how it goes. You're using Python, right?
>
> Getting the Linux version to run without the GTK installed will be a
> separate task.

Yes, using Python. I didn't test the JSON-RPC yet as I don't have Bitcoin running on the vps yet. It doesn't work without a window manager even if GTK libraries are installed. I asked about it at wxWidgets forum (http://wxforum.shadonet.com/viewtopic.php?t=26954) but they didn't have much clue. Maybe we'll just need to make two different binaries.

Email #162

Date: Sun, 14 Feb 2010 19:59:12 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Exchange options

I'm moving in the direction of making transactions automated only when the customer buys coins with SMS payment provided by ZayPay. Pecunix is the only reliable and practical enough e-currency that I'd store my reserves in, but the exchange fees are quite high (about 5%).

When I'm buying coins, my recommended payment method would be IBAN transfer. I could also say "contact us if you want to buy/sell with any other payment option" and handle each order separately. I could manually accept single orders with even PayPal, as long as I don't store my money there and the customer pays the fees.

Email #163

Date: Sun, 14 Feb 2010 21:48:31 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
>> I haven't tested my JSON-RPC server with anything else yet. If you do,
>> please tell me how it goes. You're using Python, right?
>>
>> Getting the Linux version to run without the GTK installed will be a
>> separate task.
>
> Yes, using Python. I didn't test the JSON-RPC yet as I don't have
> Bitcoin running on the vps yet. It doesn't work without a window manager
> even if GTK libraries are installed. I asked about it at wxWidgets forum
> (http://wxforum.shadonet.com/viewtopic.php?t=26954) but they didn't have
> much clue. Maybe we'll just need to make two different binaries.

I will probably relent and do that. I can move init and shutdown into
init.cpp or start.cpp or something, link only wxbase and not link ui.o
and uibase.o.

wxWidgets is mostly Windows people, they wouldn't know much about GTK.

Don't you have an Ubuntu laptop you can test and compile on so you don't
have to toy with the vps?

Email #164

Date: Mon, 15 Feb 2010 15:00:34 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

> Don't you have an Ubuntu laptop you can test and compile on so you
> don't have to toy with the vps?

Yes. Tested with Python's JSON-RPC, and seems to work fine! Really
easy to use.

Email #165

Date: Mon, 15 Feb 2010 18:11:53 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
>> Don't you have an Ubuntu laptop you can test and compile on so you
>> don't have to toy with the vps?
>
> Yes. Tested with Python's JSON-RPC, and seems to work fine! Really easy
> to use.

Hurray, I got it on the first go.

Could you send me the Python code you used? So if I do some testing
later I don't have to figure it out myself.

Email #166

Date: Mon, 15 Feb 2010 20:33:23 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

> mmalmi@cc.hut.fi wrote:
>>> Don't you have an Ubuntu laptop you can test and compile on so you
>>> don't have to toy with the vps?
>>
>> Yes. Tested with Python's JSON-RPC, and seems to work fine! Really
>> easy to use.

>
> Hurray, I got it on the first go.
>
> Could you send me the Python code you used? So if I do some testing
> later I don't have to figure it out myself.

Just downloaded the python-json-rpc
(http://json-rpc.org/wiki/python-json-rpc) from their svn and tested
by talking to the Python interpreter directly. Like this:

```
pythons = ServiceProxy("http://localhost:8332")
s.getblockcount()
```

Email #167

Date: Wed, 17 Feb 2010 19:32:04 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Non-GUI option

Just a few clues I've found about running the same binary without a GUI:

1) GTK supports running a program without display:
http://library.gnome.org/devel/gtk/2.12/gtk-General.html#gtk-init-check. This
doesn't tell if it's possible in wxWidgets though.

2) wxAppConsole of wx 2.9 might be useful somehow. Just replacing
wxApp with wxAppConsole doesn't work, I'm not sure how it should be
used. It's not very well documented.

3) Another option might be to use IMPLEMENT_APP_NO_MAIN() and make our
own main method.

Email #168

Date: Mon, 22 Feb 2010 20:17:42 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Non-GUI option

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> Just a few clues I've found about running the same binary without a GUI:
>
> 1) GTK supports running a program without display:
> http://library.gnome.org/devel/gtk/2.12/gtk-General.html#gtk-init-check.
> This doesn't tell if it's possible in wxWidgets though.

I see it calls gtk-init-check in wxApp::Initialize.

I can subclass Initialize, call the original one while suppressing the
error message and ignore the return value. It seems to be working.

Any suggestions what to name the command line switches and how to
describe them? Is there any traditional standard? I'm currently using:
-daemon (or -d)   (Enables RPC and runs in the background)
-server   (Enables RPC)

Email #169

Date: Tue, 23 Feb 2010 01:41:01 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Non-GUI option
To: Martti Malmi <mmalmi@cc.hut.fi>

>> Just a few clues I've found about running the same binary without a GUI:
>>
>> 1) GTK supports running a program without display:
>> http://library.gnome.org/devel/gtk/2.12/gtk-General.html#gtk-init-check.
>> This doesn't tell if it's possible in wxWidgets though.
>
> I see it calls gtk-init-check in wxApp::Initialize.
>
> I can subclass Initialize, call the original one while suppressing the
> error message and ignore the return value. It seems to be working.

This is working. A few more things and I'll upload it.

We'll need to tell people to install the GTK libraries. Do you remember
the apt-get command to install GTK, and can you install it without
having a GUI installed?

Email #170

Date: Tue, 23 Feb 2010 15:19:51 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Non-GUI option

> mmalmi@cc.hut.fi wrote:
>> Just a few clues I've found about running the same binary without a GUI:
>>
>> 1) GTK supports running a program without display:
>> http://library.gnome.org/devel/gtk/2.12/gtk-General.html#gtk-init-check.
>> This doesn't tell if it's possible in wxWidgets though.
>
> I see it calls gtk-init-check in wxApp::Initialize.
>
> I can subclass Initialize, call the original one while suppressing the
> error message and ignore the return value. It seems to be working.
>
> Any suggestions what to name the command line switches and how to
> describe them? Is there any traditional standard? I'm currently using:
> -daemon (or -d)   (Enables RPC and runs in the background)
> -server   (Enables RPC)

That seems good, I don't know of any standards about it.

Email #171

Date: Tue, 23 Feb 2010 16:47:59 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Non-GUI option

>>> Just a few clues I've found about running the same binary without a GUI:
>>>
>>> 1) GTK supports running a program without display:
>>> http://library.gnome.org/devel/gtk/2.12/gtk-General.html#gtk-init-check.
>>> This doesn't tell if it's possible in wxWidgets though.
>>
>> I see it calls gtk-init-check in wxApp::Initialize.
>>

>> I can subclass Initialize, call the original one while suppressing
>> the error message and ignore the return value. It seems to be
>> working.
>
> This is working. A few more things and I'll upload it.
>
> We'll need to tell people to install the GTK libraries. Do you
> remember the apt-get command to install GTK, and can you install it
> without having a GUI installed?

It was probably apt-get install libgtk2.0-0. You can search for
available packages like this: "apt-cache search libgtk".

I'll give Drupal accounts to the bitcoin.org translators, so they can
keep the translations up to date.

Email #172

Date: Wed, 24 Feb 2010 06:34:52 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Non-GUI option

To: mmalmi@cc.hut.fi

> I'll give Drupal accounts to the bitcoin.org translators, so they can
> keep the translations up to date.

Good, that gives them a little sense of ownership and responsibility.

I hope we get at least one .mo file for the software translation in time
to put into the 0.3 release.

Email #173

Date: Sun, 28 Feb 2010 06:12:44 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Bitcoind

I tried debugging my build of bitcoind with ddd debugger, but didn't
have much success yet. It always ends up taking all the system's
memory and finally crashes. Could you please send me again the latest

64 bit build of bitcoind, so I can see if the problem is about my build?

Email #174

Date: Sun, 28 Feb 2010 14:47:01 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

I put it at bitcoin.org/download/linux64-0.2.7.1.tar.gz. You can delete it when you've got it.

I thought about what might cause the problem you're having and made a change that this build includes. This might have been unsafe code, although it would probably always get lucky.

in util.cpp, old:

```
const char* wxGetTranslation(const char* pszEnglish)
{
    // Wrapper of wxGetTranslation returning the same const char* type as was passed in
    static CCriticalSection cs;
    CRITICAL_BLOCK(cs)
    {
        // Look in cache
        static map<string, char*> mapCache;
        map<string, char*>::iterator mi = mapCache.find(pszEnglish);
        if (mi != mapCache.end())
            return (*mi).second;

        // wxWidgets translation
        const char* pszTranslated = wxGetTranslation(wxString(pszEnglish, wxConvUTF8)).utf8_str();

        // We don't cache unknown strings because caller might be passing in a
        // dynamic string and we would keep allocating memory for each variation.
        if (strcmp(pszEnglish, pszTranslated) == 0)
            return pszEnglish;

        // Add to cache, memory doesn't need to be freed.  We only
```

```
cache because
        // we must pass back a pointer to permanently allocated memory.
        char* pszCached = new char[strlen(pszTranslated)+1];
        strcpy(pszCached, pszTranslated);
        mapCache[pszEnglish] = pszCached;
        return pszCached;
    }
    return NULL;
}

new:
const char* wxGetTranslation(const char* pszEnglish)
{
    // Wrapper of wxGetTranslation returning the same const char* type
as was passed in
    static CCriticalSection cs;
    CRITICAL_BLOCK(cs)
    {
        // Look in cache
        static map<string, char*> mapCache;
        map<string, char*>::iterator mi = mapCache.find(pszEnglish);
        if (mi != mapCache.end())
            return (*mi).second;

        // wxWidgets translation
        wxString strTranslated = wxGetTranslation(wxString(pszEnglish,
wxConvUTF8));

        // We don't cache unknown strings because caller might be
passing in a
        // dynamic string and we would keep allocating memory for each
variation.
        if (strcmp(pszEnglish, strTranslated.utf8_str()) == 0)
            return pszEnglish;

        // Add to cache, memory doesn't need to be freed.  We only
cache because
        // we must pass back a pointer to permanently allocated memory.
        char* pszCached = new char[strlen(strTranslated.utf8_str())+1];
        strcpy(pszCached, strTranslated.utf8_str());
        mapCache[pszEnglish] = pszCached;
        return pszCached;
    }
```

```
     return NULL;
}

If you still suspect this code, for testing you could change it to:
const char* wxGetTranslation(const char* pszEnglish)
{
     return pszEnglish;
}


mmalmi@cc.hut.fi wrote:
> I tried debugging my build of bitcoind with ddd debugger, but didn't
> have much success yet. It always ends up taking all the system's memory
> and finally crashes. Could you please send me again the latest 64 bit
> build of bitcoind, so I can see if the problem is about my build?
>
```

Email #175

Date: Sun, 28 Feb 2010 20:09:07 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

```
Could you send me the debug.log?

mmalmi@cc.hut.fi wrote:
> I tried debugging my build of bitcoind with ddd debugger, but didn't
> have much success yet. It always ends up taking all the system's memory
> and finally crashes. Could you please send me again the latest 64 bit
> build of bitcoind, so I can see if the problem is about my build?
>
```

Email #176

Date: Tue, 02 Mar 2010 21:33:24 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

Here goes. I forgot to mention the crash error message:

terminate called after throwing an instance of 'std::bad_alloc'
what(): std::bad_alloc

> Could you send me the debug.log?
>
> mmalmi@cc.hut.fi wrote:
>> I tried debugging my build of bitcoind with ddd debugger, but
>> didn't have much success yet. It always ends up taking all the
>> system's memory and finally crashes. Could you please send me again
>> the latest 64 bit build of bitcoind, so I can see if the problem
>> is about my build?
>>

Email #177

Date: Tue, 02 Mar 2010 21:36:10 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

This was from the compilation you sent, the same problem occurred with it.

> Here goes. I forgot to mention the crash error message:
>
> terminate called after throwing an instance of 'std::bad_alloc'
> what(): std::bad_alloc
>
>> Could you send me the debug.log?
>>
>> mmalmi@cc.hut.fi wrote:
>>> I tried debugging my build of bitcoind with ddd debugger, but
>>> didn't have much success yet. It always ends up taking all the
>>> system's memory and finally crashes. Could you please send me
>>> again the latest 64 bit build of bitcoind, so I can see if the
>>> problem is about my build?
>>>

Email #178

Date: Tue, 02 Mar 2010 22:27:22 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoind
To: mmalmi@cc.hut.fi

Does it still do it if you didn't do getinfo?

You could comment out the CreateThreads listed below, then re-enable
them one at a time until it does it again. Then we would know which
thread the problem is in.

net.cpp, under // Start threads
    CreateThread(ThreadIRCSeed, NULL)
    CreateThread(ThreadSocketHandler, NULL, true)
    CreateThread(ThreadOpenConnections, NULL)
    CreateThread(ThreadMessageHandler, NULL)

init.cpp:
    CreateThread(ThreadRPCServer, NULL);

mmalmi@cc.hut.fi wrote:
> Here goes. I forgot to mention the crash error message:
>
> terminate called after throwing an instance of 'std::bad_alloc'
> what(): std::bad_alloc
>
>> Could you send me the debug.log?
>>
>> mmalmi@cc.hut.fi wrote:
>>> I tried debugging my build of bitcoind with ddd debugger, but didn't
>>> have much success yet. It always ends up taking all the system's
>>> memory and finally crashes. Could you please send me again the
>>> latest 64 bit build of bitcoind, so I can see if the problem is
>>> about my build?
>>>
>
>

>

Email #179

Date: Wed, 03 Mar 2010 03:50:39 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

I get the error regardless of the getinfo. Commenting out
ThreadIRCSeed fixed the problem.

> Does it still do it if you didn't do getinfo?
>
> You could comment out the CreateThreads listed below, then re-enable
> them one at a time until it does it again. Then we would know which
> thread the problem is in.
>
> net.cpp, under // Start threads
>   CreateThread(ThreadIRCSeed, NULL)
>   CreateThread(ThreadSocketHandler, NULL, true)
>   CreateThread(ThreadOpenConnections, NULL)
>   CreateThread(ThreadMessageHandler, NULL)
>
> init.cpp:
>   CreateThread(ThreadRPCServer, NULL);
>
> mmalmi@cc.hut.fi wrote:
>> Here goes. I forgot to mention the crash error message:
>>
>> terminate called after throwing an instance of 'std::bad_alloc'
>> what(): std::bad_alloc
>>
>>> Could you send me the debug.log?
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>> didn't have much success yet. It always ends up taking all the
>>>> system's memory and finally crashes. Could you please send me
>>>> again the latest 64 bit build of bitcoind, so I can see if the
>>>> problem is about my build?
>>>>

>>
>>
>>

Email #180

Date: Wed, 03 Mar 2010 03:54:52 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

That narrows it down a lot. It didn't print any IRC activity in
debug.log, so I guess it couldn't have gotten past the RecvUntil.
Eyeballing it I don't see anything obvious. I guess it would have to be
either in ConnectSocket or RecvUntil.

Try it with the attached irc.cpp and net.cpp and send me the debug.log.

Or you could run it in gdb and step through ThreadIRCSeed
gdb --args bitcoin [switches]
b ThreadIRCSeed
run
step
or u to step over and up out of routines.

mmalmi@cc.hut.fi wrote:
> I get the error regardless of the getinfo. Commenting out ThreadIRCSeed
> fixed the problem.
>
>> Does it still do it if you didn't do getinfo?
>>
>> You could comment out the CreateThreads listed below, then re-enable
>> them one at a time until it does it again. Then we would know which
>> thread the problem is in.
>>
>> net.cpp, under // Start threads
>> CreateThread(ThreadIRCSeed, NULL)
>> CreateThread(ThreadSocketHandler, NULL, true)
>> CreateThread(ThreadOpenConnections, NULL)
>> CreateThread(ThreadMessageHandler, NULL)

>>
>> init.cpp:
>>   CreateThread(ThreadRPCServer, NULL);
>>
>> mmalmi@cc.hut.fi wrote:
>>> Here goes. I forgot to mention the crash error message:
>>>
>>> terminate called after throwing an instance of 'std::bad_alloc'
>>> what(): std::bad_alloc
>>>
>>>> Could you send me the debug.log?
>>>>
>>>> mmalmi@cc.hut.fi wrote:
>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>> didn't have much success yet. It always ends up taking all the
>>>>> system's memory and finally crashes. Could you please send me
>>>>> again the latest 64 bit build of bitcoind, so I can see if the
>>>>> problem is about my build?
>>>>>
>>>
>>>
>>>
>
>
>

Email #181

Date: Wed, 03 Mar 2010 14:32:01 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

debug.log attached

> That narrows it down a lot. It didn't print any IRC activity in
> debug.log, so I guess it couldn't have gotten past the RecvUntil.
> Eyeballing it I don't see anything obvious. I guess it would have to
> be either in ConnectSocket or RecvUntil.
>
> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>

> Or you could run it in gdb and step through ThreadIRCSeed
> gdb --args bitcoin [switches]
> b ThreadIRCSeed
> run
> step
> or u to step over and up out of routines.
>
> mmalmi@cc.hut.fi wrote:
>> I get the error regardless of the getinfo. Commenting out
>> ThreadIRCSeed fixed the problem.
>>
>>> Does it still do it if you didn't do getinfo?
>>>
>>> You could comment out the CreateThreads listed below, then re-enable
>>> them one at a time until it does it again. Then we would know which
>>> thread the problem is in.
>>>
>>> net.cpp, under // Start threads
>>>   CreateThread(ThreadIRCSeed, NULL)
>>>   CreateThread(ThreadSocketHandler, NULL, true)
>>>   CreateThread(ThreadOpenConnections, NULL)
>>>   CreateThread(ThreadMessageHandler, NULL)
>>>
>>> init.cpp:
>>>   CreateThread(ThreadRPCServer, NULL);
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> Here goes. I forgot to mention the crash error message:
>>>>
>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>> what(): std::bad_alloc
>>>>
>>>>> Could you send me the debug.log?
>>>>>
>>>>> mmalmi@cc.hut.fi wrote:
>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>> didn't have much success yet. It always ends up taking all the
>>>>>>   system's memory and finally crashes. Could you please send
>>>>>> me   again the latest 64 bit build of bitcoind, so I can see
>>>>>> if the   problem is about my build?
>>>>>>
>>>>
>>>>

>>>>
>>
>>
>>

Email #182

Date: Wed, 03 Mar 2010 17:15:28 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoind
To: mmalmi@cc.hut.fi

It's in RecvUntil, but I still can't see anything wrong with it. The only thing I can think of is if the socket is receiving a spew of characters.

Try this irc.cpp. debug.log may grow rapidly so be ready to kill it.

mmalmi@cc.hut.fi wrote:
> debug.log attached
>
>> That narrows it down a lot. It didn't print any IRC activity in
>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>> Eyeballing it I don't see anything obvious. I guess it would have to
>> be either in ConnectSocket or RecvUntil.
>>
>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>
>> Or you could run it in gdb and step through ThreadIRCSeed
>> gdb --args bitcoin [switches]
>> b ThreadIRCSeed
>> run
>> step
>> or u to step over and up out of routines.
>>
>> mmalmi@cc.hut.fi wrote:
>>> I get the error regardless of the getinfo. Commenting out
>>> ThreadIRCSeed fixed the problem.
>>>
>>>> Does it still do it if you didn't do getinfo?

>>>>
>>>> You could comment out the CreateThreads listed below, then re-enable
>>>> them one at a time until it does it again. Then we would know which
>>>> thread the problem is in.
>>>>
>>>> net.cpp, under // Start threads
>>>>   CreateThread(ThreadIRCSeed, NULL)
>>>>   CreateThread(ThreadSocketHandler, NULL, true)
>>>>   CreateThread(ThreadOpenConnections, NULL)
>>>>   CreateThread(ThreadMessageHandler, NULL)
>>>>
>>>> init.cpp:
>>>>   CreateThread(ThreadRPCServer, NULL);
>>>>
>>>> mmalmi@cc.hut.fi wrote:
>>>>> Here goes. I forgot to mention the crash error message:
>>>>>
>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>> what(): std::bad_alloc
>>>>>
>>>>>> Could you send me the debug.log?
>>>>>>
>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>> didn't have much success yet. It always ends up taking all the
>>>>>>>   system's memory and finally crashes. Could you please send
>>>>>>> me   again the latest 64 bit build of bitcoind, so I can see if
>>>>>>> the   problem is about my build?
>>>>>>>
>>>>>
>>>>>
>>>>>
>>>
>>>
>>>
>
>
>

Email #183

Date: Fri, 05 Mar 2010 00:27:08 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

Here's the debug.log. I stopped bitcoind before it took up all the memory.

> It's in RecvUntil, but I still can't see anything wrong with it. The
> only thing I can think of is if the socket is receiving a spew of
> characters.
>
> Try this irc.cpp. debug.log may grow rapidly so be ready to kill it.
>
> mmalmi@cc.hut.fi wrote:
>> debug.log attached
>>
>>> That narrows it down a lot. It didn't print any IRC activity in
>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>>> Eyeballing it I don't see anything obvious. I guess it would have to
>>> be either in ConnectSocket or RecvUntil.
>>>
>>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>>
>>> Or you could run it in gdb and step through ThreadIRCSeed
>>> gdb --args bitcoin [switches]
>>> b ThreadIRCSeed
>>> run
>>> step
>>> or u to step over and up out of routines.
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> I get the error regardless of the getinfo. Commenting out
>>>> ThreadIRCSeed fixed the problem.
>>>>
>>>>> Does it still do it if you didn't do getinfo?
>>>>>
>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>> them one at a time until it does it again. Then we would know which
>>>>> thread the problem is in.
>>>>>
>>>>> net.cpp, under // Start threads
>>>>> CreateThread(ThreadIRCSeed, NULL)
>>>>> CreateThread(ThreadSocketHandler, NULL, true)
>>>>> CreateThread(ThreadOpenConnections, NULL)

>>>>> CreateThread(ThreadMessageHandler, NULL)
>>>>>
>>>>> init.cpp:
>>>>> CreateThread(ThreadRPCServer, NULL);
>>>>>
>>>>> mmalmi@cc.hut.fi wrote:
>>>>>> Here goes. I forgot to mention the crash error message:
>>>>>>
>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>> what(): std::bad_alloc
>>>>>>
>>>>>>> Could you send me the debug.log?
>>>>>>>
>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>>> didn't have much success yet. It always ends up taking
>>>>>>>> all the system's memory and finally crashes. Could you
>>>>>>>> please send me again the latest 64 bit build of bitcoind,
>>>>>>>> so I can see if the problem is about my build?
>>>>>>>>
>>>>>>
>>>>>>
>>>>>>
>>>>
>>>>
>>>>
>>
>>
>>

Email #184

Date: Fri, 05 Mar 2010 02:09:02 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

Here's another test run debug.log I got when debugging with gdb. The program started eating memory after the debug line "irc 8" and within a few seconds crashed with "terminate called after throwing an

instance of 'std::bad_alloc'".

> It's in RecvUntil, but I still can't see anything wrong with it. The
> only thing I can think of is if the socket is receiving a spew of
> characters.
>
> Try this irc.cpp. debug.log may grow rapidly so be ready to kill it.
>
> mmalmi@cc.hut.fi wrote:
>> debug.log attached
>>
>>> That narrows it down a lot. It didn't print any IRC activity in
>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>>> Eyeballing it I don't see anything obvious. I guess it would have to
>>> be either in ConnectSocket or RecvUntil.
>>>
>>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>>
>>> Or you could run it in gdb and step through ThreadIRCSeed
>>> gdb --args bitcoin [switches]
>>> b ThreadIRCSeed
>>> run
>>> step
>>> or u to step over and up out of routines.
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> I get the error regardless of the getinfo. Commenting out
>>>> ThreadIRCSeed fixed the problem.
>>>>
>>>>> Does it still do it if you didn't do getinfo?
>>>>>
>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>> them one at a time until it does it again. Then we would know which
>>>>> thread the problem is in.
>>>>>
>>>>> net.cpp, under // Start threads
>>>>> CreateThread(ThreadIRCSeed, NULL)
>>>>> CreateThread(ThreadSocketHandler, NULL, true)
>>>>> CreateThread(ThreadOpenConnections, NULL)
>>>>> CreateThread(ThreadMessageHandler, NULL)
>>>>>
>>>>> init.cpp:
>>>>> CreateThread(ThreadRPCServer, NULL);

>>>>>
>>>>> mmalmi@cc.hut.fi wrote:
>>>>>> Here goes. I forgot to mention the crash error message:
>>>>>>
>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>> what(): std::bad_alloc
>>>>>>
>>>>>>> Could you send me the debug.log?
>>>>>>>
>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>>>   didn't have much success yet. It always ends up taking
>>>>>>>> all the   system's memory and finally crashes. Could you
>>>>>>>> please send me   again the latest 64 bit build of bitcoind,
>>>>>>>> so I can see if the problem is about my build?
>>>>>>>>
>>>>>>
>>>>>>
>>>>>>
>>>>
>>>>
>>>>
>>
>>
>>

Email #185

Date: Fri, 05 Mar 2010 00:42:16 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

It's in util.c ParseString. I'm guessing the problem is incompatibility between the type "unsigned int" and the type of str.npos, which is size_type.

Try changing the two "unsigned int"s to "size_type".

old:

```
void ParseString(const string& str, char c, vector<string>& v)
{
     unsigned int i1 = 0;
     unsigned int i2;
     do
     {
         i2 = str.find(c, i1);
         v.push_back(str.substr(i1, i2-i1));
         i1 = i2+1;
     }
     while (i2 != str.npos);
}

new:
void ParseString(const string& str, char c, vector<string>& v)
{
     size_type i1 = 0;
     size_type i2;
     do
     {
         i2 = str.find(c, i1);
         v.push_back(str.substr(i1, i2-i1));
         i1 = i2+1;
     }
     while (i2 != str.npos);
}



mmalmi@cc.hut.fi wrote:
> Here's another test run debug.log I got when debugging with gdb. The
> program started eating memory after the debug line "irc 8" and within a
> few seconds crashed with "terminate called after throwing an instance of
> 'std::bad_alloc'".
>
>> It's in RecvUntil, but I still can't see anything wrong with it.  The
>> only thing I can think of is if the socket is receiving a spew of
>> characters.
>>
>> Try this irc.cpp.  debug.log may grow rapidly so be ready to kill it.
>>
>> mmalmi@cc.hut.fi wrote:
>>> debug.log attached
>>>
```

>>>> That narrows it down a lot. It didn't print any IRC activity in
>>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>>>> Eyeballing it I don't see anything obvious. I guess it would have to
>>>> be either in ConnectSocket or RecvUntil.
>>>>
>>>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>>>
>>>> Or you could run it in gdb and step through ThreadIRCSeed
>>>> gdb --args bitcoin [switches]
>>>> b ThreadIRCSeed
>>>> run
>>>> step
>>>> or u to step over and up out of routines.
>>>>
>>>> mmalmi@cc.hut.fi wrote:
>>>>> I get the error regardless of the getinfo. Commenting out
>>>>> ThreadIRCSeed fixed the problem.
>>>>>
>>>>>> Does it still do it if you didn't do getinfo?
>>>>>>
>>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>>> them one at a time until it does it again. Then we would know which
>>>>>> thread the problem is in.
>>>>>>
>>>>>> net.cpp, under // Start threads
>>>>>>   CreateThread(ThreadIRCSeed, NULL)
>>>>>>   CreateThread(ThreadSocketHandler, NULL, true)
>>>>>>   CreateThread(ThreadOpenConnections, NULL)
>>>>>>   CreateThread(ThreadMessageHandler, NULL)
>>>>>>
>>>>>> init.cpp:
>>>>>>   CreateThread(ThreadRPCServer, NULL);
>>>>>>
>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>> Here goes. I forgot to mention the crash error message:
>>>>>>>
>>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>>> what(): std::bad_alloc
>>>>>>>
>>>>>>>> Could you send me the debug.log?
>>>>>>>>
>>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but

>>>>>>>>> didn't have much success yet. It always ends up taking all
>>>>>>>>> the system's memory and finally crashes. Could you please
>>>>>>>>> send me again the latest 64 bit build of bitcoind, so I can
>>>>>>>>> see if the problem is about my build?
>>>>>>>>>
>>>>>>>
>>>>>>>
>>>>>>>
>>>>>
>>>>>
>>>>>
>>>
>>>
>>>
>
>
>

Email #186

Date: Fri, 05 Mar 2010 00:54:40 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

Actually, please try this instead, this is more correct:

```
void ParseString(const string& str, char c, vector<string>& v)
{
    string::size_type i1 = 0;
    string::size_type i2;
    loop
    {
        i2 = str.find(c, i1);
        if (i2 == str.npos)
        {
            v.push_back(str.substr(i1));
            return;
        }
        v.push_back(str.substr(i1, i2-i1));
        i1 = i2+1;
    }
```

```
}
```

Satoshi Nakamoto wrote:

```
> It's in util.c ParseString.  I'm guessing the problem is incompatibility
> between the type "unsigned int" and the type of str.npos, which is
> size_type.
>
> Try changing the two "unsigned int"s to "size_type".
>
> old:
> void ParseString(const string& str, char c, vector<string>& v)
> {
>     unsigned int i1 = 0;
>     unsigned int i2;
>     do
>     {
>         i2 = str.find(c, i1);
>         v.push_back(str.substr(i1, i2-i1));
>         i1 = i2+1;
>     }
>     while (i2 != str.npos);
> }
>
> new:
> void ParseString(const string& str, char c, vector<string>& v)
> {
>     size_type i1 = 0;
>     size_type i2;
>     do
>     {
>         i2 = str.find(c, i1);
>         v.push_back(str.substr(i1, i2-i1));
>         i1 = i2+1;
>     }
>     while (i2 != str.npos);
> }
>
>
> mmalmi@cc.hut.fi wrote:
>> Here's another test run debug.log I got when debugging with gdb. The
>> program started eating memory after the debug line "irc 8" and within
```

>> a few seconds crashed with "terminate called after throwing an
>> instance of 'std::bad_alloc'".
>>
>>> It's in RecvUntil, but I still can't see anything wrong with it. The
>>> only thing I can think of is if the socket is receiving a spew of
>>> characters.
>>>
>>> Try this irc.cpp. debug.log may grow rapidly so be ready to kill it.
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> debug.log attached
>>>>
>>>>> That narrows it down a lot. It didn't print any IRC activity in
>>>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>>>>> Eyeballing it I don't see anything obvious. I guess it would have to
>>>>> be either in ConnectSocket or RecvUntil.
>>>>>
>>>>> Try it with the attached irc.cpp and net.cpp and send me the
>>>>> debug.log.
>>>>>
>>>>> Or you could run it in gdb and step through ThreadIRCSeed
>>>>> gdb --args bitcoin [switches]
>>>>> b ThreadIRCSeed
>>>>> run
>>>>> step
>>>>> or u to step over and up out of routines.
>>>>>
>>>>> mmalmi@cc.hut.fi wrote:
>>>>>> I get the error regardless of the getinfo. Commenting out
>>>>>> ThreadIRCSeed fixed the problem.
>>>>>>
>>>>>>> Does it still do it if you didn't do getinfo?
>>>>>>>
>>>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>>>> them one at a time until it does it again. Then we would know which
>>>>>>> thread the problem is in.
>>>>>>>
>>>>>>> net.cpp, under // Start threads
>>>>>>> CreateThread(ThreadIRCSeed, NULL)
>>>>>>> CreateThread(ThreadSocketHandler, NULL, true)
>>>>>>> CreateThread(ThreadOpenConnections, NULL)
>>>>>>> CreateThread(ThreadMessageHandler, NULL)
>>>>>>>

>>>>>>> init.cpp:
>>>>>>> CreateThread(ThreadRPCServer, NULL);
>>>>>>>
>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>> Here goes. I forgot to mention the crash error message:
>>>>>>>>
>>>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>>>> what(): std::bad_alloc
>>>>>>>>
>>>>>>>>> Could you send me the debug.log?
>>>>>>>>>
>>>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>>>>>   didn't have much success yet. It always ends up taking
>>>>>>>>>> all the system's memory and finally crashes. Could you
>>>>>>>>>> please send me again the latest 64 bit build of bitcoind,
>>>>>>>>>> so I can see if the problem is about my build?
>>>>>>>>>>
>>>>>>>>
>>>>>>>>
>>>>>>>>
>>>>>>
>>>>>>
>>>>>>
>>>>
>>>>
>>>>
>>
>>
>>
>

Email #187

Date: Fri, 05 Mar 2010 03:33:34 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

Great! Works fine now.

```
> Actually, please try this instead, this is more correct:
>
> void ParseString(const string& str, char c, vector<string>& v)
> {
>     string::size_type i1 = 0;
>     string::size_type i2;
>     loop
>     {
>         i2 = str.find(c, i1);
>         if (i2 == str.npos)
>         {
>             v.push_back(str.substr(i1));
>             return;
>         }
>         v.push_back(str.substr(i1, i2-i1));
>         i1 = i2+1;
>     }
> }
>
>
>
> Satoshi Nakamoto wrote:
>> It's in util.c ParseString.  I'm guessing the problem is
>> incompatibility between the type "unsigned int" and the type of
>> str.npos, which is size_type.
>>
>> Try changing the two "unsigned int"s to "size_type".
>>
>> old:
>> void ParseString(const string& str, char c, vector<string>& v)
>> {
>>    unsigned int i1 = 0;
>>    unsigned int i2;
>>    do
>>    {
>>        i2 = str.find(c, i1);
>>        v.push_back(str.substr(i1, i2-i1));
>>        i1 = i2+1;
>>    }
>>    while (i2 != str.npos);
>> }
>>
>> new:
```

```
>> void ParseString(const string& str, char c, vector<string>& v)
>> {
>>    size_type i1 = 0;
>>    size_type i2;
>>    do
>>    {
>>        i2 = str.find(c, i1);
>>        v.push_back(str.substr(i1, i2-i1));
>>        i1 = i2+1;
>>    }
>>    while (i2 != str.npos);
>> }
>>
>>
>> mmalmi@cc.hut.fi wrote:
>>> Here's another test run debug.log I got when debugging with gdb.
>>> The program started eating memory after the debug line "irc 8" and
>>>  within a few seconds crashed with "terminate called after
>>> throwing  an instance of 'std::bad_alloc'".
>>>
>>>> It's in RecvUntil, but I still can't see anything wrong with it.  The
>>>> only thing I can think of is if the socket is receiving a spew of
>>>> characters.
>>>>
>>>> Try this irc.cpp.  debug.log may grow rapidly so be ready to kill it.
>>>>
>>>> mmalmi@cc.hut.fi wrote:
>>>>> debug.log attached
>>>>>
>>>>>> That narrows it down a lot.  It didn't print any IRC activity in
>>>>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>>>>>> Eyeballing it I don't see anything obvious.  I guess it would have to
>>>>>> be either in ConnectSocket or RecvUntil.
>>>>>>
>>>>>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>>>>>
>>>>>> Or you could run it in gdb and step through ThreadIRCSeed
>>>>>> gdb --args bitcoin [switches]
>>>>>> b ThreadIRCSeed
>>>>>> run
>>>>>> step
>>>>>> or u to step over and up out of routines.
>>>>>>
```

>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>> I get the error regardless of the getinfo. Commenting out
>>>>>>> ThreadIRCSeed fixed the problem.
>>>>>>>
>>>>>>>> Does it still do it if you didn't do getinfo?
>>>>>>>>
>>>>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>>>>> them one at a time until it does it again. Then we would know which
>>>>>>>> thread the problem is in.
>>>>>>>>
>>>>>>>> net.cpp, under // Start threads
>>>>>>>> CreateThread(ThreadIRCSeed, NULL)
>>>>>>>> CreateThread(ThreadSocketHandler, NULL, true)
>>>>>>>> CreateThread(ThreadOpenConnections, NULL)
>>>>>>>> CreateThread(ThreadMessageHandler, NULL)
>>>>>>>>
>>>>>>>> init.cpp:
>>>>>>>> CreateThread(ThreadRPCServer, NULL);
>>>>>>>>
>>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>>> Here goes. I forgot to mention the crash error message:
>>>>>>>>>
>>>>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>>>>> what(): std::bad_alloc
>>>>>>>>>
>>>>>>>>>> Could you send me the debug.log?
>>>>>>>>>>
>>>>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>>>>> I tried debugging my build of bitcoind with ddd debugger,
>>>>>>>>>>> but   didn't have much success yet. It always ends up
>>>>>>>>>>> taking all the   system's memory and finally crashes.
>>>>>>>>>>> Could you please send me   again the latest 64 bit build
>>>>>>>>>>> of bitcoind, so I can see if the problem is about my
>>>>>>>>>>> build?
>>>>>>>>>>>
>>>>>>>>>
>>>>>>>>>
>>>>>>>>>
>>>>>>>
>>>>>>>
>>>>>>>
>>>>>
>>>>>

>>>>>
>>>
>>>
>>>
>>
>>

Email #188

Date: Fri, 05 Mar 2010 01:42:00 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

I confirmed that ParseString has this problem, and uploaded the fixed
util.cpp to SVN.

string::npos == -1

Comparing unsigned int -1 (0xffffffff) with long unsigned int -1
(0xffffffffffffffff) results in the unsigned int being promoted to
64-bit, which is 0x00000000ffffffff != 0xffffffffffffffff.

mmalmi@cc.hut.fi wrote:
> Here's another test run debug.log I got when debugging with gdb. The
> program started eating memory after the debug line "irc 8" and within a
> few seconds crashed with "terminate called after throwing an instance of
> 'std::bad_alloc'".
>
>> It's in RecvUntil, but I still can't see anything wrong with it. The
>> only thing I can think of is if the socket is receiving a spew of
>> characters.
>>
>> Try this irc.cpp. debug.log may grow rapidly so be ready to kill it.
>>
>> mmalmi@cc.hut.fi wrote:
>>> debug.log attached
>>>
>>>> That narrows it down a lot. It didn't print any IRC activity in
>>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.

>>>> Eyeballing it I don't see anything obvious. I guess it would have to
>>>> be either in ConnectSocket or RecvUntil.
>>>>
>>>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>>>
>>>> Or you could run it in gdb and step through ThreadIRCSeed
>>>> gdb --args bitcoin [switches]
>>>> b ThreadIRCSeed
>>>> run
>>>> step
>>>> or u to step over and up out of routines.
>>>>
>>>> mmalmi@cc.hut.fi wrote:
>>>>> I get the error regardless of the getinfo. Commenting out
>>>>> ThreadIRCSeed fixed the problem.
>>>>>
>>>>>> Does it still do it if you didn't do getinfo?
>>>>>>
>>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>>> them one at a time until it does it again. Then we would know which
>>>>>> thread the problem is in.
>>>>>>
>>>>>> net.cpp, under // Start threads
>>>>>>   CreateThread(ThreadIRCSeed, NULL)
>>>>>>   CreateThread(ThreadSocketHandler, NULL, true)
>>>>>>   CreateThread(ThreadOpenConnections, NULL)
>>>>>>   CreateThread(ThreadMessageHandler, NULL)
>>>>>>
>>>>>> init.cpp:
>>>>>>   CreateThread(ThreadRPCServer, NULL);
>>>>>>
>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>> Here goes. I forgot to mention the crash error message:
>>>>>>>
>>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>>> what(): std::bad_alloc
>>>>>>>
>>>>>>>> Could you send me the debug.log?
>>>>>>>>
>>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>>>>   didn't have much success yet. It always ends up taking all
>>>>>>>>> the   system's memory and finally crashes. Could you please

>>>>>>>>> send me again the latest 64 bit build of bitcoind, so I can
>>>>>>>>> see if the problem is about my build?
>>>>>>>>>
>>>>>>>
>>>>>>>
>>>>>>>
>>>>>
>>>>>
>>>>>
>>>
>>>
>>>
>
>
>

Email #189

Date: Sat, 06 Mar 2010 06:39:53 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Blog

To: Martti Malmi <mmalmi@cc.hut.fi>

There's a blog writer who wants to write a story about Bitcoin, but I don't have time right now to answer his questions. Would you be interested in answering his questions if I refer him to you? We might get a good link out of it.

The blog is
http://themonetaryfuture.blogspot.com

Email #190

Date: Sun, 07 Mar 2010 02:46:35 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Blog

Yes, I could do that.

> There's a blog writer who wants to write a story about Bitcoin, but I

> don't have time right now to answer his questions. Would you be
> interested in answering his questions if I refer him to you? We might
> get a good link out of it.
>
> The blog is
> http://themonetaryfuture.blogspot.com

Email #191

Date: Fri, 14 May 2010 09:16:52 +0300

From: mmalmi@cc.hut.fi

To: satoshin@gmx.com

Subject: Status update

Hi!

How are you doing? Haven't seen you around in a while.

I've been at full-time work lately, and will be until the end of June, so I haven't had that much time to work with Bitcoin or my exchange service. I have a working beta of my service though, and a few weeks ago made my first transaction: sold 10,000 btc for 20 euros via EU bank transfer. Maybe I can make it public soon.

I divided the forum into 6 boards, which are Bitcoin Discussion, Development & Technical Discussion, Technical support, Economics, Marketplace and Trading Discussion. Hope this is ok?

I also added a page "Trade" on the bitcoin.org site, where btc-accepting services are listed. It's nice to see that there are already useful services that accept btc.

The community has been growing nicely. We've had around 10-20 people and active discussion at #bitcoin-dev lately.

It would be nice to get the daemon-able binaries to SF.net. We have some skilled programmers in the community now, so maybe we can finish the JSON API functions if you don't have time to.

Best regards.

Email #192

Date: Sun, 16 May 2010 20:12:21 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Status update

To: mmalmi@cc.hut.fi

I've also been busy with other things for the last month and a half. I just now downloaded my e-mail since the beginning of April. I mostly have things sorted and should be back to Bitcoin shortly. Glad that you've been handling things in my absence. Congrats on your first transaction!

As I recall, the code was nearly ready for a 0.3 release. I think all it needed was a little testing time and to install the new icon xpm.

The JSON API functions are complete. I wanted to take another fresh look at them in case I think of any better function names before committing. I ought to write some sample code showing the proper way to use them, particularly with polling for received transactions. When I left off, I was thinking about bolting a payment mechanism onto a free upload server software as an example. It would make sense to actually build one practical application with the API before releasing it. You don't realise the problems with an API until you actually try to use it.

mmalmi@cc.hut.fi wrote:
> Hi!
>
> How are you doing? Haven't seen you around in a while.
>
> I've been at full-time work lately, and will be until the end of June,
> so I haven't had that much time to work with Bitcoin or my exchange
> service. I have a working beta of my service though, and a few weeks ago
> made my first transaction: sold 10,000 btc for 20 euros via EU bank
> transfer. Maybe I can make it public soon.
>
> I divided the forum into 6 boards, which are Bitcoin Discussion,
> Development & Technical Discussion, Technical support, Economics,
> Marketplace and Trading Discussion. Hope this is ok?
>

> I also added a page "Trade" on the bitcoin.org site, where btc-accepting
> services are listed. It's nice to see that there are already useful
> services that accept btc.
>
> The community has been growing nicely. We've had around 10-20 people and
> active discussion at #bitcoin-dev lately.
>
> It would be nice to get the daemon-able binaries to SF.net. We have some
> skilled programmers in the community now, so maybe we can finish the
> JSON API functions if you don't have time to.
>
> Best regards.
>

Email #193

Date: Tue, 22 Jun 2010 18:36:22 +0100
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: 0.3.0 rc1 quickie download link
To: Martti Malmi <mmalmi@cc.hut.fi>

If bandwidth is a problem, delete my link in the "0.3 almost ready"
thread. I just don't want to upload it to sourceforge for a quickie
share for a day or two, possibly taking it down immediately if there's a
bug. Sourceforge has a policy of not allowing removal of files once
they're added, and it's a pain to upload to. I'll delete the file once
the release is ready.

BTW, it's looking like I may be able to get us some money soon to cover
web host costs, back your exchange service, etc, in the form of cash in
the mail. Can you receive it and act as the project's treasurer?

Email #194

Date: Tue, 22 Jun 2010 21:51:21 +0300
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: 0.3.0 rc1 quickie download link

> If bandwidth is a problem, delete my link in the "0.3 almost ready"
> thread. I just don't want to upload it to sourceforge for a quickie

> share for a day or two, possibly taking it down immediately if there's
> a bug. Sourceforge has a policy of not allowing removal of files once
> they're added, and it's a pain to upload to. I'll delete the file once
> the release is ready.

Ok, I'll monitor it. Bandwidth hasn't been a problem so far - it's
been about 2 GB (0.5 dollars) per month at most. Other costs are about
15$ a month.

> BTW, it's looking like I may be able to get us some money soon to cover
> web host costs, back your exchange service, etc, in the form of cash in
> the mail. Can you receive it and act as the project's treasurer?

That would be nice, I can do it. Sending cash in the mail may have its
risks, but maybe it's still the best anonymous option. We can also ask
for donations in BTC on the forum.

Email #195

Date: Wed, 23 Jun 2010 21:33:57 +0100
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: donation
To: mmalmi@cc.hut.fi

>> BTW, it's looking like I may be able to get us some money soon to cover
>> web host costs, back your exchange service, etc, in the form of cash in
>> the mail. Can you receive it and act as the project's treasurer?
>
> That would be nice, I can do it. Sending cash in the mail may have its
> risks, but maybe it's still the best anonymous option. We can also ask
> for donations in BTC on the forum.

I got a donation offer for $2000 USD. I need to get your postal mailing
address to have him send to. And yes, he wants to remain anonymous, so
please keep the envelope's origin private.

Email #196

Date: Fri, 25 Jun 2010 08:55:14 +0300
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: donation

You can give this address:

Martti Malmi
Visakoivunkuja 15 F 42
02130 Espoo
Finland

>>> BTW, it's looking like I may be able to get us some money soon to cover
>>> web host costs, back your exchange service, etc, in the form of cash in
>>> the mail. Can you receive it and act as the project's treasurer?
>>
>> That would be nice, I can do it. Sending cash in the mail may have
>> its risks, but maybe it's still the best anonymous option. We can
>> also ask for donations in BTC on the forum.
>
> I got a donation offer for $2000 USD. I need to get your postal
> mailing address to have him send to. And yes, he wants to remain
> anonymous, so please keep the envelope's origin private.

Email #197

Date: Tue, 06 Jul 2010 03:59:57 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Anonymous, homepage changes

To: Martti Malmi <mmalmi@cc.hut.fi>

I think we should de-emphasize the anonymous angle. With the popularity
of bitcoin addresses instead of sending by IP, we can't give the
impression it's automatically anonymous. It's possible to be
pseudonymous, but you have to be careful. If someone digs through the
transaction history and starts exposing information people thought was
anonymous, the backlash will be much worse if we haven't prepared
expectations by warning in advance that you have to take precautions if
you really want to make that work. Like Tor says, "Tor does not
magically encrypt all of your Internet activities. Understand what Tor
does and does not do for you."

Also, anonymous sounds a bit shady. I think the people who want anonymous will still figure it out without us trumpeting it.

I made some changes to the bitcoin.org homepage. It's not really crucial to update the translations. I tend to keep editing and correcting for some time afterwards, so if they want to update, they should wait.

I removed the word "anonymous", and the sentence about "anonymity means", although you worded it so carefully "...CAN be kept hidden..." it was a shame to remove it.

Instead, I added Tor instructions at the bottom, with instructions for how to stay anonymous (pseudonymous) directly after the Tor instructions: "If you want to remain anonymous (pseudonymous, really), be careful not to reveal any information linking your bitcoin addresses to your identity, and use a new bitcoin address for each payment you receive."

It helps that it can now seed automatically through Tor.

Even though it doesn't say anonymous until the bottom, I think anonymous seekers would already suspect it based on all the other attributes like no central authority to take your ID info and the way bitcoin addresses look.

Email #198

Date: Tue, 06 Jul 2010 19:03:50 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: 0.3.0 released

To: Martti Malmi <mmalmi@cc.hut.fi>

I uploaded 0.3.0 beta to sourceforge and updated the links on bitcoin.org. I still need to post the announcement message on the forum and mailing list. Here's what I've prepared:

Announcing version 0.3 of Bitcoin, the P2P cryptocurrency! Bitcoin is a digital currency using cryptography and a distributed network to replace the need for a trusted central server. Escape the arbitrary inflation

risk of centrally managed currencies! Bitcoin's total circulation is limited to 21 million coins. The coins are gradually being released to the networks nodes based on the CPU power they contribute. You can get a share of them just by installing the software and contributing your idle CPU time.

What's new:
- Command line and JSON-RPC control
- Includes a daemon version without GUI
- Tabs for sent and received transactions
- 20% faster hashing
- Hashmeter performance display
- Mac OS X version (thanks to Laszlo)
- German, Dutch and Italian translations (thanks to DataWraith, Xunie and Joozero)

Email #199

Date: Tue, 06 Jul 2010 19:40:11 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: 0.3.0 released

To: Martti Malmi <mmalmi@cc.hut.fi>

Actually, "tabs for sent and received transactions" sounds really immature if it doesn't have that already. "Transaction filter tabs" sounds better.

I'm still editing it a little more and then I'll e-mail it to bitcoin-list and send it to the cryptography list.

"Get it at http://www.bitcoin.org or read the forum to find out more."

Satoshi Nakamoto wrote:
> I uploaded 0.3.0 beta to sourceforge and updated the links on
> bitcoin.org. I still need to post the announcement message on the forum
> and mailing list. Here's what I've prepared:
>
> Announcing version 0.3 of Bitcoin, the P2P cryptocurrency! Bitcoin is a
> digital currency using cryptography and a distributed network to replace
> the need for a trusted central server. Escape the arbitrary inflation
> risk of centrally managed currencies! Bitcoin's total circulation is
> limited to 21 million coins. The coins are gradually being released to
> the networks nodes based on the CPU power they contribute. You can get

> a share of them just by installing the software and contributing your
> idle CPU time.
>
> What's new:
> - Command line and JSON-RPC control
> - Includes a daemon version without GUI
> - Tabs for sent and received transactions
> - 20% faster hashing
> - Hashmeter performance display
> - Mac OS X version (thanks to Laszlo)
> - German, Dutch and Italian translations (thanks to DataWraith, Xunie
> and Joozero)
>

Email #200

Date: Tue, 06 Jul 2010 22:53:07 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: [bitcoin-list] Bitcoin 0.3 released!

To: bitcoin-list@lists.sourceforge.net

Announcing version 0.3 of Bitcoin, the P2P cryptocurrency! Bitcoin is a digital currency using cryptography and a distributed network to replace the need for a trusted central server. Escape the arbitrary inflation risk of centrally managed currencies! Bitcoin's total circulation is limited to 21 million coins. The coins are gradually released to the network's nodes based on the CPU power they contribute, so you can get a share of them by contributing your idle CPU time.

What's new:
- Command line and JSON-RPC control
- Includes a daemon version without GUI
- Transaction filter tabs
- 20% faster hashing
- Hashmeter performance display
- Mac OS X version (thanks to Laszlo)
- German, Dutch and Italian translations (thanks to DataWraith, Xunie and Joozero)

Get it at www.bitcoin.org, and read the forum to find out more.

_____

Email #201

Date: Wed, 07 Jul 2010 01:17:54 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Anonymous, homepage changes

Ok, that sounds reasonable.

> I think we should de-emphasize the anonymous angle. With the
> popularity of bitcoin addresses instead of sending by IP, we can't give
> the impression it's automatically anonymous. It's possible to be
> pseudonymous, but you have to be careful. If someone digs through the
> transaction history and starts exposing information people thought was
> anonymous, the backlash will be much worse if we haven't prepared
> expectations by warning in advance that you have to take precautions if
> you really want to make that work. Like Tor says, "Tor does not
> magically encrypt all of your Internet activities. Understand what Tor
> does and does not do for you."
>
> Also, anonymous sounds a bit shady. I think the people who want
> anonymous will still figure it out without us trumpeting it.
>
> I made some changes to the bitcoin.org homepage. It's not really
> crucial to update the translations. I tend to keep editing and
> correcting for some time afterwards, so if they want to update, they
> should wait.
>
> I removed the word "anonymous", and the sentence about "anonymity
> means", although you worded it so carefully "...CAN be kept hidden..."
> it was a shame to remove it.
>
> Instead, I added Tor instructions at the bottom, with instructions for
> how to stay anonymous (pseudonymous) directly after the Tor

> instructions: "If you want to remain anonymous (pseudonymous, really),
> be careful not to reveal any information linking your bitcoin addresses
> to your identity, and use a new bitcoin address for each payment you
> receive."
>
> It helps that it can now seed automatically through Tor.
>
> Even though it doesn't say anonymous until the bottom, I think
> anonymous seekers would already suspect it based on all the other
> attributes like no central authority to take your ID info and the way
> bitcoin addresses look.

Email #202

Date: Wed, 14 Jul 2010 22:52:46 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Fwd: Re: bitcoin!!!!

To: Martti Malmi <mmalmi@cc.hut.fi>

I see the interior pages of the old sourceforge wiki are still up,
though the homepage forwards.

-------- Original Message --------
Subject: Re: bitcoin!!!!
Date: Wed, 14 Jul 2010 10:56:21 -0400
From: Sam <samm@sammaloney.com>
To: Satoshi Nakamoto <satoshin@gmx.com>
References: <201004111508.52168.samm@sammaloney.com>
<201007111859.29171.samm@sammaloney.com> <4C3DCD97.8030003@gmx.com>

It was an old FAQ on sourceforge that had been linked from slashdot (on a
highly visible comment). people were going there because bitcoin.org was
down
for a while.

http://bitcoin.sourceforge.net/wiki/index.php?page=FAQ

Probably not an issue anymore, but might be a good idea to delete or update
that wiki page.

> I don't see any 0.1.5 download links on the FAQ. Do you mean
> bitcoin.org/faq? Is it on one of the other languages? Or maybe someone
> else fixed it already.
>
> > Anyways, I write to you now to let you know you must update the FAQ
> > immediately. It points to 0.15 of bitcoin for download. You must update
> > it to 0.30, as it is slashdotted!
>

Email #203

Date: Thu, 15 Jul 2010 18:41:10 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: bitcoin.org drupal users

To: Martti Malmi <mmalmi@cc.hut.fi>

Is it possible for the translators (at least the more trusted ones) to have user accounts on drupal so they can update their translated text directly? The user accounts on drupal appear to be pretty weak. I created a satoshi account and it can't even edit the side bar stuff, just the main text of pages. I don't think user accounts can access any of the admin stuff. Do you think it's safe, or do you feel insecure about doing that? If you're worried, maybe there's a way to lock just the english version of the homepage.

It would be nice if when I need to make changes to the homepage, I could enlist someone like Xunie to do the rote work of reflecting it to all the translations instead of having to do all that work myself. (many light changes don't require understanding the language to fix the translated pages)

Email #204

Date: Thu, 15 Jul 2010 18:43:55 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Fwd: Please update the bitcoin FAQ so new member can have the right info

To: Martti Malmi <mmalmi@cc.hut.fi>

-------- Original Message --------
Subject: Please update the bitcoin FAQ so new member can have the right

info
Date: Mon, 12 Jul 2010 14:13:20 -0700
From: Jim Nguyen <jimmy.winn@gmail.com>
To: satoshin@gmx.com

Hi,

In the FAQ of bitcoin.org <http://bitcoin.org> the backing up of the wallet had old instructions, right? Should it just be to back up wallat.dat instead of the entire folder??? See below.

"How do I backup my wallet?

Your data is stored in the directory ''%appdata%\Bitcoin'', which is typically:

Windows XP:
C:\Documents and Settings\username\Application Data\Bitcoin
Windows Vista:
C:\Users\username\AppData\Roaming\Bitcoin

It's recommended that you stop Bitcoin before backing it up to make sure the backup will be correct."

Email #205

Date: Thu, 15 Jul 2010 21:00:12 +0100
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: bitcoin.org server
To: Martti Malmi <mmalmi@cc.hut.fi>

You did some research when choosing hosting, this was a well chosen one, right? It seems like it would be a tremendous hassle to change, and we've had good luck with this one. Cheaper will usually have some offsetting drawback in quality.

I wonder if that extra memory is just disk cache or something.

I take it you haven't received anything from that donor yet? He seemed

pretty certain he was going to send it, maybe more. (if you get anything, we need to keep private for him the fact that we got a donation)

Email #206

Date: Sat, 17 Jul 2010 04:27:38 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: bitcoin.org drupal users

Yes, we could give accounts to trusted translators. I haven't found a way to give them edit permissions to only one page, but they can be forced to create a new revision with every page change they make, and not be allowed to delete revisions. Xunie would be the first on the list I'd give an account. :)

> Is it possible for the translators (at least the more trusted ones) to
> have user accounts on drupal so they can update their translated text
> directly? The user accounts on drupal appear to be pretty weak. I
> created a satoshi account and it can't even edit the side bar stuff,
> just the main text of pages. I don't think user accounts can access
> any of the admin stuff. Do you think it's safe, or do you feel
> insecure about doing that? If you're worried, maybe there's a way to
> lock just the english version of the homepage.
>
> It would be nice if when I need to make changes to the homepage, I
> could enlist someone like Xunie to do the rote work of reflecting it to
> all the translations instead of having to do all that work myself.
> (many light changes don't require understanding the language to fix the
> translated pages)

Email #207

Date: Sat, 17 Jul 2010 04:33:46 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fwd: Re: bitcoin!!!!

Relocated the old site to /oldsite, now there's only the redirection.

> I see the interior pages of the old sourceforge wiki are still up,
> though the homepage forwards.
>
>
> -------- Original Message --------
> Subject: Re: bitcoin!!!!
> Date: Wed, 14 Jul 2010 10:56:21 -0400
> From: Sam <samm@sammaloney.com>
> To: Satoshi Nakamoto <satoshin@gmx.com>
> References: <201004111508.52168.samm@sammaloney.com>
> <201007111859.29171.samm@sammaloney.com> <4C3DCD97.8030003@gmx.com>
>
> It was an old FAQ on sourceforge that had been linked from slashdot (on a
> highly visible comment). people were going there because bitcoin.org was down
> for a while.
>
> http://bitcoin.sourceforge.net/wiki/index.php?page=FAQ
>
> Probably not an issue anymore, but might be a good idea to delete or update
> that wiki page.
>
>> I don't see any 0.1.5 download links on the FAQ. Do you mean
>> bitcoin.org/faq? Is it on one of the other languages? Or maybe someone
>> else fixed it already.
>>
>>> Anyways, I write to you now to let you know you must update the FAQ
>>> immediately. It points to 0.15 of bitcoin for download. You must update
>>> it to 0.30, as it is slashdotted!
>>

Email #208

Date: Sun, 18 Jul 2010 02:21:45 +0300

From: mmalmi@cc.hut.fi

To: satoshin@gmx.com

Subject: Fwd: bitcoin hosting

Rackspace has very good support, good backend, good connections and nicely scaling cloud based virtual servers. I got this offer from Thufir:

Hi Sirius,

Check out www.citrusdesignstudio.com. You will see through the portfolio that I am a real business with many clients.

That is my business that I provide managed hosting through.
I also do unmanaged VPSes.

Normally I would charge $15/mo for 512MB.
I will do it for $10/mo for you.

To see my pricing, go to www.linnode.com. I match everything they have except their great panel -- you have to email or call my people.

I provide VPS services normally for 3/4ths the posted cost on linnode.com.
(Rackspace is even more expensive.)

I will do it for 1/2 of linnode's price for you.

It scales linerally just like linnodes, so for 2048 MB of memory, I would charge $40, etc.

Later!

That would be worth considering, if they have good datacenters and connections. $10 / month is about $20 less than what Rackspace costs. On the other hand, Rackspace prices are no problem if the donation is to arrive.

Email #209

Date: Sun, 18 Jul 2010 16:23:21 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: wiki

To: Martti Malmi <mmalmi@cc.hut.fi>

http://www.bitcoin.org/smf/index.php?topic=393.msg3785#msg3785

AndrewBuck:
...

EDIT: The wiki doesn't seem to be sending the registration e-mail so I can log in to edit, is there some problem with the server or something?

-Buck

Email #210

Date: Sun, 18 Jul 2010 16:23:10 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fwd: bitcoin hosting

To: mmalmi@cc.hut.fi

Please promise me you won't make a switch now. The last thing we need is switchover hassle on top of the slashdot flood of work we've got now. I'm losing my mind there are so many things that need to be done.

Also, it would suck to be on a smaller, less reliable host just to save a measly $20.

I will try to think of a polite way to ask the donor if he sent it, but right now there are other higher priority things that are going to bump even that for a few days.

Would a donation of bitcoins help in the short term?

mmalmi@cc.hut.fi wrote:
> Rackspace has very good support, good backend, good connections and
> nicely scaling cloud based virtual servers. I got this offer from Thufir:
>
> -----
> Hi Sirius,
>
> Check out www.citrusdesignstudio.com. You will see through the portfolio
> that
> I am a real business with many clients.
>

> That is my business that I provide managed hosting through.
> I also do unmanaged VPSes.
>
> Normally I would charge $15/mo for 512MB.
> I will do it for $10/mo for you.
>
> To see my pricing, go to www.linnode.com. I match everything they have
> except
> their great panel -- you have to email or call my people.
>
> I provide VPS services normally for 3/4ths the posted cost on linnode.com.
> (Rackspace is even more expensive.)
>
> I will do it for 1/2 of linnode's price for you.
>
> It scales linerally just like linnodes, so for 2048 MB of memory, I would
> charge $40, etc.
>
> Later!
> -----
>
> That would be worth considering, if they have good datacenters and
> connections. $10 / month is about $20 less than what Rackspace costs. On
> the other hand, Rackspace prices are no problem if the donation is to
> arrive.
>

Email #211

Date: Mon, 19 Jul 2010 02:51:11 +0300
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Fwd: bitcoin hosting

Ok, I won't switch it. Donations in Bitcoin are helpful and can be
sent to 14EXchS9j3AAfim6mL4jtw6VWMosSUiG5U.

> Please promise me you won't make a switch now. The last thing we need
> is switchover hassle on top of the slashdot flood of work we've got
> now. I'm losing my mind there are so many things that need to be done.
>
> Also, it would suck to be on a smaller, less reliable host just to save

> a measly $20.
>
> I will try to think of a polite way to ask the donor if he sent it, but
> right now there are other higher priority things that are going to bump
> even that for a few days.
>
> Would a donation of bitcoins help in the short term?
>
> mmalmi@cc.hut.fi wrote:
>> Rackspace has very good support, good backend, good connections and
>> nicely scaling cloud based virtual servers. I got this offer from
>> Thufir:
>>
>> -----
>> Hi Sirius,
>>
>> Check out www.citrusdesignstudio.com. You will see through the
>> portfolio that
>> I am a real business with many clients.
>>
>> That is my business that I provide managed hosting through.
>> I also do unmanaged VPSes.
>>
>> Normally I would charge $15/mo for 512MB.
>> I will do it for $10/mo for you.
>>
>> To see my pricing, go to www.linnode.com. I match everything they
>> have except
>> their great panel -- you have to email or call my people.
>>
>> I provide VPS services normally for 3/4ths the posted cost on linnode.com.
>> (Rackspace is even more expensive.)
>>
>> I will do it for 1/2 of linnode's price for you.
>>
>> It scales linerally just like linnodes, so for 2048 MB of memory, I would
>> charge $40, etc.
>>
>> Later!
>> -----
>>
>> That would be worth considering, if they have good datacenters and
>> connections. $10 / month is about $20 less than what Rackspace

>> costs. On the other hand, Rackspace prices are no problem if the
>> donation is to arrive.
>>

Email #212

Date: Wed, 21 Jul 2010 23:33:18 +0300
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Donation

Good news: I received the donation of $3600. At least the hosting
costs are no problem anymore.

What do you think of the idea to offer rewards of $100-200 to the
first 5-10 established companies that start accepting Bitcoin? We'd
also assign them a dedicated support person to help with integration.
I have companies like prq.se, ipredator.se, relakks.com or
perfect-privacy.com in mind. We could also make the offer public.

Email #213

Date: Wed, 21 Jul 2010 23:28:33 +0100
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Donation
To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> Good news: I received the donation of $3600. At least the hosting costs
> are no problem anymore.

That's great! I'll let him know it was received and thank him.

It might be a long time before we get another donation like that, we
should save a lot of it.

Spend what you need on hosting. Email me a simple accounting when you
take out money for expenses, like:

-$60 rackspace monthly
$2540 balance

> What do you think of the idea to offer rewards of $100-200 to the first
> 5-10 established companies that start accepting Bitcoin? We'd also
> assign them a dedicated support person to help with integration. I have
> companies like prq.se, ipredator.se, relakks.com or perfect-privacy.com
> in mind. We could also make the offer public.

$100-200 is chump change if they're a serious company, it would only make us sound small.

What they need most is confidence they can convert it to fiat currency. That VOIP company essentially said so in a recent post. The best thing we can do is make sure there's cash available to cash out and support and steady the conversion rate.

The money is leveraged better that way too. Theoretically, imagine 10 businesses have their eye on a $100 bill being offered for bitcoins, but don't actually cash out because they know it's there if they need it. That one $100 bill allowed 10 different people to act like their 5000 bitcoins were equivalent to $100.

I think we should allocate $1000 at this point to your exchange.

Email #214

Date: Fri, 23 Jul 2010 07:41:11 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Donation

> Spend what you need on hosting. Email me a simple accounting when you
> take out money for expenses, like:
> -$60 rackspace monthly
> $2540 balance

Ok.

>> What do you think of the idea to offer rewards of $100-200 to the
>> first 5-10 established companies that start accepting Bitcoin? We'd

>> also assign them a dedicated support person to help with
>> integration. I have companies like prq.se, ipredator.se,
>> relakks.com or perfect-privacy.com in mind. We could also make the
>> offer public.
>
> $100-200 is chump change if they're a serious company, it would only
> make us sound small.
>
> What they need most is confidence they can convert it to fiat currency.
> That VOIP company essentially said so in a recent post. The best
> thing we can do is make sure there's cash available to cash out and
> support and steady the conversion rate.
>
> The money is leveraged better that way too. Theoretically, imagine 10
> businesses have their eye on a $100 bill being offered for bitcoins,
> but don't actually cash out because they know it's there if they need
> it. That one $100 bill allowed 10 different people to act like their
> 5000 bitcoins were equivalent to $100.
>
> I think we should allocate $1000 at this point to your exchange.

Alright, I'll add $1000 dollars to the exchange reserves. That way I
can offer more stable pricing.

A week ago somebody bought coins with 1000 €. That was probably meant
as a donation to some extent, since 1000 € would have bought him a lot
more coins at bitcoinmarket.com than at my service.

Email #215

Date: Fri, 23 Jul 2010 16:59:42 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Donation

To: mmalmi@cc.hut.fi

>> I think we should allocate $1000 at this point to your exchange.
>
> Alright, I'll add $1000 dollars to the exchange reserves. That way I can
> offer more stable pricing.
>
> A week ago somebody bought coins with 1000 €. That was probably meant as
> a donation to some extent, since 1000 € would have bought him a lot more

> coins at bitcoinmarket.com than at my service.

Interesting, so how is the balance between purchases of coins and cash going?

Btw, are you able to use my builds of bitcoind on your host, or do you have to build it yourself?

Email #216

Date: Sat, 24 Jul 2010 07:32:37 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Donation

> Interesting, so how is the balance between purchases of coins and cash going?

About +1000€ (plus the $1000) and -40000 BTC since when I started. I should have set the initial BTC price higher, it was only 1€ / 1000 BTC in the beginning.

> Btw, are you able to use my builds of bitcoind on your host, or do you
> have to build it yourself?

I had to build it myself. It had the same problem that has been reported on the forums: /usr/lib/libstdc++.so.6: version `GLIBCXX_3.4.11' not found.

Email #217

Date: Sat, 24 Jul 2010 15:38:53 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Donation

To: mmalmi@cc.hut.fi

> A week ago somebody bought coins with 1000 €. That was probably meant as
> a donation to some extent, since 1000 € would have bought him a lot more
> coins at bitcoinmarket.com than at my service.

They probably couldn't have gotten that large of a trade on bitcoinmarket.com.

Email #218

Date: Mon, 26 Jul 2010 19:22:08 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: /usr/lib/libstdc++.so.6: version `GLIBCXX_3.4.11'

To: mmalmi@cc.hut.fi

>> Btw, are you able to use my builds of bitcoind on your host, or do you
>> have to build it yourself?
>
> I had to build it myself. It had the same problem that has been reported
> on the forums: /usr/lib/libstdc++.so.6: version `GLIBCXX_3.4.11' not found.

Wish I could figure out how to fix that. What version of GLIBCXX does your system have?

Make sure you upgrade to Bitcoin 0.3.3 as soon as possible.

Email #219

Date: Thu, 29 Jul 2010 03:18:56 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Forum e-mail notifications and PBL blacklist and wiki registration

To: Martti Malmi <mmalmi@cc.hut.fi>

http://www.bitcoin.org/smf/index.php?topic=338.0

> of e-mail blackhole list or at least the ISP that hosts the e-mail server for registration is on one of those lists.
>
> "Looks like bitcoin.org is listed on the PBL."
> http://www.spamhaus.org/pbl/query/PBL340779

I think our problem may be that we have forum notifications on, like e-mail you when you receive a PM, but we don't have e-mail verification of new accounts. Can someone put someone else's e-mail address without verifying it, then have stuff sent there? We need to stop that right away before it gets used for something bad. Either disallow all

notification, or make sure e-mail addresses are verified.

I'm more inclined to disallow notifications or anything where the forum sends you e-mail. I kinda like not requiring e-mail verification. But if that's the only way to make sure we don't send e-mails to un-verified addresses, then we could do that.

If we request to get off of PBL, we'd better make sure we've got the problem secured first.

I changed Registration->settings->registration of new members to "Member Activation". I assume that means it e-mail verifies.
"Member Activation
When this option is enabled any members registering to the forum will have a activation link emailed to them which they must click before they can become full members"

I think that's the only way to make sure the forum can't be used to send to other people's e-mail addresses and potentially use it to spam.

Email #220

Date: Fri, 30 Jul 2010 06:34:38 +0100
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: [bitcoin-list] Alert: upgrade to bitcoin 0.3.6
To: bitcoin-list@lists.sourceforge.net

Please upgrade to 0.3.6 ASAP to get an important bugfix.

See the bitcoin.org homepage for download links.

Email #221

Date: Mon, 02 Aug 2010 21:56:06 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: [Fwd: no activation mail]

To: Martti Malmi <mmalmi@cc.hut.fi>

Oh great, now we're screwed.

We probably got spam blocked because we were allowing registrations without e-mail verification. But now that we've enabled it, our verification e-mails are blocked.

There could still be some existing user accounts created before the registration requirement being used by spammers.

We're kind of in a jam here. Can you make sure there's nothing else you can think of that might be acting as an open e-mail gateway or way for spammers to use our system for putting out spam? Check the e-mail logs and see if there's been a lot of traffic and what it's from. If you can figure out what the problem was and shut it down, then after you're sure it's fixed, request PBL to take us off the block list.

If there's a way to prohibit the forum from sending e-mail notifications, maybe we should do that.

-------- Original Message --------
Subject: no activation mail
Date: Mon, 02 Aug 2010 22:30:35 +0200
From: Youri <youri.de.bruycker@telenet.be>
To: satoshin@gmx.com

Hey Satoshin,

I tried to register me at the bitcoinforum, but I didn't get an activation mail.
Tried the resend activation code option a few times, changed the mailadress from my telenet to my gmail and back, but no luck. Looked at my spam folder but it's not there. So I guess something went wrong, could you activate my account?

My username is Skull88.

Thanks in advance,
Youri

Email #222

Date: Mon, 02 Aug 2010 22:08:22 +0100
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Disabled some notifications
To: Martti Malmi <mmalmi@cc.hut.fi>

For "normal members" I disabled "Request notification on replies" and
"Request notification on new topics".

I'm pretty sure there's a notification option for when you receive PMs,
but I don't see a way to disable it. If we have to, I guess we could
edit the php code.

Email #223

Date: Mon, 02 Aug 2010 22:09:20 +0100
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: [Fwd: Forum e-mail notifications and PBL blacklist and wiki registration]
To: Martti Malmi <mmalmi@cc.hut.fi>

Here's the info about PBL again.

-------- Original Message --------
Subject: Forum e-mail notifications and PBL blacklist and wiki registration
Date: Thu, 29 Jul 2010 03:18:56 +0100
From: Satoshi Nakamoto <satoshin@gmx.com>
To: Martti Malmi <mmalmi@cc.hut.fi>

http://www.bitcoin.org/smf/index.php?topic=338.0

> of e-mail blackhole list or at least the ISP that hosts the e-mail server for
registration is on one of those lists.
>
> "Looks like bitcoin.org is listed on the PBL."

> http://www.spamhaus.org/pbl/query/PBL340779

I think our problem may be that we have forum notifications on, like e-mail you when you receive a PM, but we don't have e-mail verification of new accounts. Can someone put someone else's e-mail address without verifying it, then have stuff sent there? We need to stop that right away before it gets used for something bad. Either disallow all notification, or make sure e-mail addresses are verified.

I'm more inclined to disallow notifications or anything where the forum sends you e-mail. I kinda like not requiring e-mail verification. But if that's the only way to make sure we don't send e-mails to un-verified addresses, then we could do that.

If we request to get off of PBL, we'd better make sure we've got the problem secured first.

I changed Registration->settings->registration of new members to "Member Activation". I assume that means it e-mail verifies.
"Member Activation
When this option is enabled any members registering to the forum will have a activation link emailed to them which they must click before they can become full members"

I think that's the only way to make sure the forum can't be used to send to other people's e-mail addresses and potentially use it to spam.

Email #224

Date: Wed, 04 Aug 2010 00:37:13 +0300
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: [Fwd: no activation mail]

The logs don't tell very much, they just confirm that many servers reject the emails sent by our server. I can't think of anything other than pm notifications that could have caused the spam listing. I'll check if I can disable the notifications from the code.

We can allow registrations without email confirmation. It's no problem when we're already on the spam list and no problem after the notifications are disabled.

> Oh great, now we're screwed.
>
> We probably got spam blocked because we were allowing registrations
> without e-mail verification. But now that we've enabled it, our
> verification e-mails are blocked.
>
> There could still be some existing user accounts created before the
> registration requirement being used by spammers.
>
> We're kind of in a jam here. Can you make sure there's nothing else
> you can think of that might be acting as an open e-mail gateway or way
> for spammers to use our system for putting out spam? Check the e-mail
> logs and see if there's been a lot of traffic and what it's from. If
> you can figure out what the problem was and shut it down, then after
> you're sure it's fixed, request PBL to take us off the block list.
>
> If there's a way to prohibit the forum from sending e-mail
> notifications, maybe we should do that.
>
>
>
> -------- Original Message --------
> Subject: no activation mail
> Date: Mon, 02 Aug 2010 22:30:35 +0200
> From: Youri <youri.de.bruycker@telenet.be>
> To: satoshin@gmx.com
>
> Hey Satoshin,
>
> I tried to register me at the bitcoinforum, but I didn't get an activation
> mail.
> Tried the resend activation code option a few times, changed the
> mailadress from my telenet to my gmail and back, but no luck. Looked at my
> spam folder but it's not there. So I guess something went wrong, could you
> activate my account?
>
> My username is Skull88.
>
> Thanks in advance,
> Youri

Email #225

Date: Thu, 05 Aug 2010 20:03:11 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: [Fwd: no activation mail]

I edited the forum code, it shouldn't send notifications anymore.

> Oh great, now we're screwed.
>
> We probably got spam blocked because we were allowing registrations
> without e-mail verification. But now that we've enabled it, our
> verification e-mails are blocked.
>
> There could still be some existing user accounts created before the
> registration requirement being used by spammers.
>
> We're kind of in a jam here. Can you make sure there's nothing else
> you can think of that might be acting as an open e-mail gateway or way
> for spammers to use our system for putting out spam? Check the e-mail
> logs and see if there's been a lot of traffic and what it's from. If
> you can figure out what the problem was and shut it down, then after
> you're sure it's fixed, request PBL to take us off the block list.
>
> If there's a way to prohibit the forum from sending e-mail
> notifications, maybe we should do that.
>
>
>
> -------- Original Message --------
> Subject: no activation mail
> Date: Mon, 02 Aug 2010 22:30:35 +0200
> From: Youri <youri.de.bruycker@telenet.be>
> To: satoshin@gmx.com
>
> Hey Satoshin,
>
> I tried to register me at the bitcoinforum, but I didn't get an activation
> mail.

> Tried the resend activation code option a few times, changed the
> mailadress from my telenet to my gmail and back, but no luck. Looked at my
> spam folder but it's not there. So I guess something went wrong, could you
> activate my account?
>
> My username is Skull88.
>
> Thanks in advance,
> Youri

Email #226

Date: Tue, 10 Aug 2010 04:28:38 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: [Fwd: Forum e-mail notifications and PBL blacklist and wiki registration]

I sent a removal request to PBL.

The FAQ says: "The first thing to know is: THE PBL IS NOT A BLACKLIST.
You are not listed for spamming or for anything you have done. The PBL
is simply a list of all of the world's dynamic IP space, i.e: IP
ranges normally assigned to ISP broadband customers (DSL, DHCP, PPP,
cable, dialup). It is perfectly normal for dynamic IP addresses to be
listed on the PBL. In fact all dynamic IP addresses in the world
should be on the PBL. Even static IPs which do not send mail should be
listed in the PBL." So we didn't even need to allow spam to be on the
list.

> Here's the info about PBL again.
>
>
> -------- Original Message --------
> Subject: Forum e-mail notifications and PBL blacklist and wiki registration
> Date: Thu, 29 Jul 2010 03:18:56 +0100
> From: Satoshi Nakamoto <satoshin@gmx.com>
> To: Martti Malmi <mmalmi@cc.hut.fi>
>
> http://www.bitcoin.org/smf/index.php?topic=338.0
>

>> of e-mail blackhole list or at least the ISP that hosts the e-mail
>> server for registration is on one of those lists.
>>
>> "Looks like bitcoin.org is listed on the PBL."
>> http://www.spamhaus.org/pbl/query/PBL340779
>
> I think our problem may be that we have forum notifications on, like
> e-mail you when you receive a PM, but we don't have e-mail verification
> of new accounts. Can someone put someone else's e-mail address without
> verifying it, then have stuff sent there? We need to stop that right
> away before it gets used for something bad. Either disallow all
> notification, or make sure e-mail addresses are verified.
>
> I'm more inclined to disallow notifications or anything where the forum
> sends you e-mail. I kinda like not requiring e-mail verification. But
> if that's the only way to make sure we don't send e-mails to un-verified
> addresses, then we could do that.
>
> If we request to get off of PBL, we'd better make sure we've got the
> problem secured first.
>
> I changed Registration->settings->registration of new members to "Member
> Activation". I assume that means it e-mail verifies.
> "Member Activation
> When this option is enabled any members registering to the forum will
> have a activation link emailed to them which they must click before they
> can become full members"
>
> I think that's the only way to make sure the forum can't be used to send
> to other people's e-mail addresses and potentially use it to spam.

Email #227

Date: Wed, 11 Aug 2010 01:19:38 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Donation

I deposited the donation to a bank as euros. The donation was actually
not $3600 but 3500$. I miscalculated it as it was packed in (18 + 17)

* $100 instead of (18 + 18) * $100.

$3500 made 2608.28€.

-750€ to back up BitcoinExchange.com
-28.92€ for the hosting in July
1829€ balance

Email #228

Date: Wed, 11 Aug 2010 02:54:27 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: [Fwd: Forum e-mail notifications and PBL blacklist and wiki registration]

To: mmalmi@cc.hut.fi

Are PM notifications still disabled? (All we really need is disable the forum's access to the mail server)

> Does it work correctly now? I had made some forum code changes to
> disable PM email notification, but just reverted most of them as
> unnecessary.

mmalmi@cc.hut.fi wrote:
> I sent a removal request to PBL.
>
> The FAQ says: "The first thing to know is: THE PBL IS NOT A BLACKLIST.
> You are not listed for spamming or for anything you have done. The PBL
> is simply a list of all of the world's dynamic IP space, i.e: IP ranges
> normally assigned to ISP broadband customers (DSL, DHCP, PPP, cable,
> dialup). It is perfectly normal for dynamic IP addresses to be listed on
> the PBL. In fact all dynamic IP addresses in the world should be on the
> PBL. Even static IPs which do not send mail should be listed in the
> PBL." So we didn't even need to allow spam to be on the list.
>
>> Here's the info about PBL again.
>>
>>
>> -------- Original Message --------
>> Subject: Forum e-mail notifications and PBL blacklist and wiki
>> registration
>> Date: Thu, 29 Jul 2010 03:18:56 +0100
>> From: Satoshi Nakamoto <satoshin@gmx.com>

>> To: Martti Malmi <mmalmi@cc.hut.fi>
>>
>> http://www.bitcoin.org/smf/index.php?topic=338.0
>>
>>> of e-mail blackhole list or at least the ISP that hosts the e-mail
>>> server for registration is on one of those lists.
>>>
>>> "Looks like bitcoin.org is listed on the PBL."
>>> http://www.spamhaus.org/pbl/query/PBL340779
>>
>> I think our problem may be that we have forum notifications on, like
>> e-mail you when you receive a PM, but we don't have e-mail verification
>> of new accounts. Can someone put someone else's e-mail address without
>> verifying it, then have stuff sent there? We need to stop that right
>> away before it gets used for something bad. Either disallow all
>> notification, or make sure e-mail addresses are verified.
>>
>> I'm more inclined to disallow notifications or anything where the forum
>> sends you e-mail. I kinda like not requiring e-mail verification. But
>> if that's the only way to make sure we don't send e-mails to un-verified
>> addresses, then we could do that.
>>
>> If we request to get off of PBL, we'd better make sure we've got the
>> problem secured first.
>>
>> I changed Registration->settings->registration of new members to "Member
>> Activation". I assume that means it e-mail verifies.
>> "Member Activation
>> When this option is enabled any members registering to the forum will
>> have a activation link emailed to them which they must click before they
>> can become full members"
>>
>> I think that's the only way to make sure the forum can't be used to send
>> to other people's e-mail addresses and potentially use it to spam.
>
>
>

Email #229

Date: Wed, 11 Aug 2010 06:42:32 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: [Fwd: Forum e-mail notifications and PBL blacklist and wiki registration]

Yes, they're still disabled. Disabling the access to the mail server
would be easy, but we probably want to keep the password recovery by
email.

> Are PM notifications still disabled? (All we really need is disable
> the forum's access to the mail server)
>
>> Does it work correctly now? I had made some forum code changes to
>> disable PM email notification, but just reverted most of them as
>> unnecessary.
>
> mmalmi@cc.hut.fi wrote:
>> I sent a removal request to PBL.
>>
>> The FAQ says: "The first thing to know is: THE PBL IS NOT A
>> BLACKLIST. You are not listed for spamming or for anything you have
>> done. The PBL is simply a list of all of the world's dynamic IP
>> space, i.e: IP ranges normally assigned to ISP broadband customers
>> (DSL, DHCP, PPP, cable, dialup). It is perfectly normal for dynamic
>> IP addresses to be listed on the PBL. In fact all dynamic IP
>> addresses in the world should be on the PBL. Even static IPs which
>> do not send mail should be listed in the PBL." So we didn't even
>> need to allow spam to be on the list.
>>
>>> Here's the info about PBL again.
>>>
>>>
>>> -------- Original Message --------
>>> Subject: Forum e-mail notifications and PBL blacklist and wiki registration
>>> Date: Thu, 29 Jul 2010 03:18:56 +0100
>>> From: Satoshi Nakamoto <satoshin@gmx.com>
>>> To: Martti Malmi <mmalmi@cc.hut.fi>
>>>
>>> http://www.bitcoin.org/smf/index.php?topic=338.0
>>>
>>>> of e-mail blackhole list or at least the ISP that hosts the
>>>> e-mail server for registration is on one of those lists.
>>>>
>>>> "Looks like bitcoin.org is listed on the PBL."
>>>> http://www.spamhaus.org/pbl/query/PBL340779

>>>
>>> I think our problem may be that we have forum notifications on, like
>>> e-mail you when you receive a PM, but we don't have e-mail verification
>>> of new accounts. Can someone put someone else's e-mail address without
>>> verifying it, then have stuff sent there? We need to stop that right
>>> away before it gets used for something bad. Either disallow all
>>> notification, or make sure e-mail addresses are verified.
>>>
>>> I'm more inclined to disallow notifications or anything where the forum
>>> sends you e-mail. I kinda like not requiring e-mail verification. But
>>> if that's the only way to make sure we don't send e-mails to un-verified
>>> addresses, then we could do that.
>>>
>>> If we request to get off of PBL, we'd better make sure we've got the
>>> problem secured first.
>>>
>>> I changed Registration->settings->registration of new members to "Member
>>> Activation". I assume that means it e-mail verifies.
>>> "Member Activation
>>> When this option is enabled any members registering to the forum will
>>> have a activation link emailed to them which they must click before they
>>> can become full members"
>>>
>>> I think that's the only way to make sure the forum can't be used to send
>>> to other people's e-mail addresses and potentially use it to spam.
>>
>>
>>

Email #230

Date: Wed, 11 Aug 2010 21:00:13 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: [Fwd: Forum e-mail notifications and PBL blacklist and wiki registration]

To: mmalmi@cc.hut.fi

Right, forgot about that.

Hopefully theymos was right that the PBL is the source of the problem.

mmalmi@cc.hut.fi wrote:
> Yes, they're still disabled. Disabling the access to the mail server
> would be easy, but we probably want to keep the password recovery by email.
>
>> Are PM notifications still disabled? (All we really need is disable
>> the forum's access to the mail server)
>>
>>> Does it work correctly now? I had made some forum code changes to
>>> disable PM email notification, but just reverted most of them as
>>> unnecessary.
>>
>> mmalmi@cc.hut.fi wrote:
>>> I sent a removal request to PBL.
>>>
>>> The FAQ says: "The first thing to know is: THE PBL IS NOT A
>>> BLACKLIST. You are not listed for spamming or for anything you have
>>> done. The PBL is simply a list of all of the world's dynamic IP
>>> space, i.e: IP ranges normally assigned to ISP broadband customers
>>> (DSL, DHCP, PPP, cable, dialup). It is perfectly normal for dynamic
>>> IP addresses to be listed on the PBL. In fact all dynamic IP
>>> addresses in the world should be on the PBL. Even static IPs which
>>> do not send mail should be listed in the PBL." So we didn't even
>>> need to allow spam to be on the list.
>>>
>>>> Here's the info about PBL again.
>>>>
>>>>
>>>> -------- Original Message --------
>>>> Subject: Forum e-mail notifications and PBL blacklist and wiki
>>>> registration
>>>> Date: Thu, 29 Jul 2010 03:18:56 +0100
>>>> From: Satoshi Nakamoto <satoshin@gmx.com>
>>>> To: Martti Malmi <mmalmi@cc.hut.fi>
>>>>
>>>> http://www.bitcoin.org/smf/index.php?topic=338.0
>>>>
>>>>> of e-mail blackhole list or at least the ISP that hosts the
>>>>> e-mail server for registration is on one of those lists.
>>>>>
>>>>> "Looks like bitcoin.org is listed on the PBL."
>>>>> http://www.spamhaus.org/pbl/query/PBL340779
>>>>
>>>> I think our problem may be that we have forum notifications on, like

>>>> e-mail you when you receive a PM, but we don't have e-mail verification
>>>> of new accounts. Can someone put someone else's e-mail address without
>>>> verifying it, then have stuff sent there? We need to stop that right
>>>> away before it gets used for something bad. Either disallow all
>>>> notification, or make sure e-mail addresses are verified.
>>>>
>>>> I'm more inclined to disallow notifications or anything where the forum
>>>> sends you e-mail. I kinda like not requiring e-mail verification. But
>>>> if that's the only way to make sure we don't send e-mails to
>>>> un-verified
>>>> addresses, then we could do that.
>>>>
>>>> If we request to get off of PBL, we'd better make sure we've got the
>>>> problem secured first.
>>>>
>>>> I changed Registration->settings->registration of new members to
>>>> "Member
>>>> Activation". I assume that means it e-mail verifies.
>>>> "Member Activation
>>>> When this option is enabled any members registering to the forum will
>>>> have a activation link emailed to them which they must click before
>>>> they
>>>> can become full members"
>>>>
>>>> I think that's the only way to make sure the forum can't be used to
>>>> send
>>>> to other people's e-mail addresses and potentially use it to spam.
>>>
>>>
>>>
>
>
>

Email #231

Date: Sun, 15 Aug 2010 21:37:28 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: [bitcoin-list] ALERT - we are investigating a problem

To: bitcoin-list@lists.sourceforge.net

*** WARNING *** We are investigating a problem. DO NOT TRUST ANY
TRANSACTIONS THAT HAPPENED AFTER 15.08.2010 17:05 UTC (block 74638)
until the issue is resolved.

_____

Email #232

Date: Fri, 27 Aug 2010 03:36:43 +0100
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: [Fwd: SweepMines now accept bitcoins]
To: Martti Malmi <mmalmi@cc.hut.fi>

-------- Original Message --------
Subject: SweepMines now accept bitcoins
Date: Tue, 24 Aug 2010 19:50:47 +0600
From: Kirill Kisel <kisel2626@gmail.com>
To: satoshin@gmx.com

Dear BitCoin.

http://apps.facebook.com/sweepmines/ now accepts BitCoins.

This is single-player computer game based on Windows Minesweeper version.

Would you be so kind to add us to the http://www.bitcoin.org/trade page?

Thank you.

Email #233

Date: Sun, 26 Sep 2010 16:27:10 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Bookkeeping

+1829€
-23,32€ August hosting bill
-24,40 September hosting bill

Email #234

Date: Sun, 26 Sep 2010 17:17:17 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bookkeeping

> +1829€
> -23,32€ August hosting bill
> -24,40 September hosting bill

+1781,28

Email #235

Date: Sun, 03 Oct 2010 21:27:29 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: SMF php code

To: Martti Malmi <mmalmi@cc.hut.fi>

I noticed my custom captcha stuff is gone. I guess it got lost in an upgrade? What are we doing for captcha now? If we only have default captcha, we'd be getting flooded with spam accounts. Do I need to re-integrate the custom captcha stuff or do we have another solution now?

Email #236

Date: Mon, 04 Oct 2010 18:41:50 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF php code

Sorry, I didn't notice your custom code when updating. Re-integration
is a good idea if it's not too much work. I've removed hundreds of
spam accounts by making a search for old accounts that have a webpage
url and 0 posts.

> I noticed my custom captcha stuff is gone. I guess it got lost in an
> upgrade? What are we doing for captcha now? If we only have default
> captcha, we'd be getting flooded with spam accounts. Do I need to
> re-integrate the custom captcha stuff or do we have another solution
> now?

Email #237

Date: Mon, 04 Oct 2010 20:05:26 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF php code

To: mmalmi@cc.hut.fi

I reuploaded the changes. For future reference, the files in Sources
with customisations are:
Register.php
PersonalMessage.php
ManageRegistration.php
Subs.php

Let me know whenever you do an upgrade so I can make sure all my changes
survived.

Hopefully the 1.1.x line is mature and updates are infrequent. We
shouldn't upgrade to 2.0. I made a ton of customisations that wouldn't
be compatible, and I kind of prefer the look of 1.1 over 2.0 anyway.

The captcha url has mycode=4 added to it, and the register page has
extra hidden mycode=2 through 5 images so any automated thing wouldn't
know which one to pick. Everything that uses captcha has to have that

mycode=4 thing added. Something in sending personal messages also uses captcha.

mmalmi@cc.hut.fi wrote:
> Sorry, I didn't notice your custom code when updating. Re-integration is
> a good idea if it's not too much work. I've removed hundreds of spam
> accounts by making a search for old accounts that have a webpage url and
> 0 posts.
>
>> I noticed my custom captcha stuff is gone. I guess it got lost in an
>> upgrade? What are we doing for captcha now? If we only have default
>> captcha, we'd be getting flooded with spam accounts. Do I need to
>> re-integrate the custom captcha stuff or do we have another solution
>> now?
>
>
>

Email #238

Date: Wed, 01 Dec 2010 00:58:37 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: [Fwd: Bitcoin.org is down]

To: Martti Malmi <mmalmi@cc.hut.fi>

-------- Original Message --------
Subject: Bitcoin.org is down
Date: Tue, 30 Nov 2010 18:27:02 -0600
From: theymos <theymos@mm.st>
To: satoshin@gmx.com

Bitcoin.org has been down for several hours.

Email #239

Date: Thu, 02 Dec 2010 22:00:56 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: What was the bitcoin.org outage?

To: Martti Malmi <mmalmi@cc.hut.fi>

Do you know what caused that outage? Did it need to be rebooted, or was it a DoS or something? The IP was pingable during the outage.

Did you get back to davidonpda about his doing a mirror backup? I think that's a really good idea. Do you do any backups, or the VPS do any for you automatically?

Email #240

Date: Fri, 03 Dec 2010 12:08:53 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: What was the bitcoin.org outage?

> Do you know what caused that outage? Did it need to be rebooted, or
> was it a DoS or something? The IP was pingable during the outage.

I don't know what it was. It started working again when I rebooted it. Someone suggested it might have been the heavy load from a Reddit post about Bitcoin. Inspecting the logs would be useful, but I don't have much time now.

> Did you get back to davidonpda about his doing a mirror backup? I
> think that's a really good idea. Do you do any backups, or the VPS do
> any for you automatically?

I told him to go ahead. I don't do automatic backups atm. We should have more server admins soon when I get bitcoinexchange.com to another server. I could give the root password to you and somebody else. Xunie has volunteered, but we might find somebody even more professional outage was due to heavy load, he could help us move to lighttpd or optimize resources otherwise. Should we make a recruitment thread on the forum?

Email #241

Date: Fri, 03 Dec 2010 19:58:40 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: What was the bitcoin.org outage?

To: mmalmi@cc.hut.fi

> I told him to go ahead. I don't do automatic backups atm. We should have
> more server admins soon when I get bitcoinexchange.com to another
> server. I could give the root password to you and somebody else. Xunie
> has volunteered, but we might find somebody even more professional from
> the forum and keep the number of admins at the minimum. If the outage
> was due to heavy load, he could help us move to lighttpd or optimize
> resources otherwise. Should we make a recruitment thread on the forum?

It should be Gavin. I trust him, he's responsible, professional, and technically much more linux capable than me.

(I don't know Xunie, but he hasn't posted for months and he was a goofball)

Email #242

Date: Mon, 06 Dec 2010 13:33:01 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: What was the bitcoin.org outage?

I'm ready to send you the password. Can you send me your PGP key so I don't have to send it in plaintext?

> It should be Gavin. I trust him, he's responsible, professional, and
> technically much more linux capable than me.

Ok, I'll ask him.

Email #243

Date: Mon, 06 Dec 2010 16:08:56 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: What was the bitcoin.org outage?

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> I'm ready to send you the password. Can you send me your PGP key so I
> don't have to send it in plaintext?
>

>> It should be Gavin. I trust him, he's responsible, professional, and
>> technically much more linux capable than me.
>
> Ok, I'll ask him.

Thanks, did you finish moving bitcoinexchange to another server?

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.7 (MingW32)

mQGiBEkJ+qcRBADKDTcZlYDRtP1Q7/ShuzBJzUh9hoVVowogf2W07U6G9BqKW24r
piOxYmErjMFfvNtozNk+33cd/sq3gi05O1IMmZzg2rbF4ne5t3iplXnNuzNh+j+6
VxxA16GPhBRprvnng8r9GYALLUpo9Xk17KE429YYKFgVvtTPtEGUlpO1EwCg7FmW
dBbRp4mn5GfxQNT1hzp9WgkD/3pZ0cB5m4enzfylOHXmRfJKBMF02ZDnsY1GqeHv
/LjkhCusTp2qz4thLycYOFKGmAddpVnMsE/TYZLgpsxjrJsrEPNSdoXk3IgEStow
mXjTfr9xNOrB20Qk0ZOO1mipOWMgse4PmIu02X24OapWtyhdHsX3oBLcwDdke8aE
gAh8A/sHlK7fL1Bi8rFzx6hb+2yIlD/fazMBVZUe0r2uo7ldqEz5+GeEiBFignd5
HHhqjJw8rUJkfeZBoTKYlDKo7XDrTRxfyzNuZZPxBLTj+keY8WgYhQ5MWsSC2MX7
FZHaJddYa0pzUmFZmQh0ydulVUQnLKzRSunsjGOnmxiWBZwb6bQjU2F0b3NoaSBO
YWthbW90byA8c2F0b3NoaW5AZ214LmNvbT6IYAQTEQIAIAUCSQn6pwIbAwYLCQgH
AwIEFQIIAwQWAgMBAh4BAheAAAoJEBjAnoZeyUihXGMAnjiWJ0fvmSgSM3o6Tu3q
RME9GN7QAKCGrFw9SUD0e9/YDcqhX1aPMrYue7kCDQRJCfqnEAgA9OTCjLa6Sj7t
dZcQxNufsDSCSB+yznIGzFGXXpJk7GgKmX3H9Zl4E6zJTQGXL2GAV4klkSfNtvgs
SGJKqCnebuZVwutyq1vXRNVFPQFvLVVo2jJCBHWjb03fmXmavIUtRCHoc8xgVJMQ
LrwvS943GgsqSbdoKZWdTnfnEq+UaGo+Qfv66NpT3Yl0CXUiNBITZOJcJdjHDTBO
XRqomX2WSguv+btYdhQGGQiaEx73XMftXNCxbOpqwsODQns7xTcl2ENru9BNIQME
I7L9FYBQUiKHm1k6RrBy1as8XElS2jEos7GAmlfF1wShFUX+NF1VOPdbN3ZdFoWq
sUjKk+QbrwADBQgA9DiD4+uuRhwk2B1TmtrXnwwhcdkE7ZbLHjxBfCsLPAZiPh8c
ICfV3S418i4H1YCz2ItcnC8KAPoS6mipyS28AU1B7zJYPODBn8E7aPSPzHJfudMK
MqiCHljVJrE23xsKTC0sIhhSKcr2G+6ARoG5lwuoqJqEyDrblVQQFpVxBNPHSTqu
O5PoLXQc7PKgC5SyQuZbEALEkItl2SL2yBRRGOlVJLnvZ6eaovkAlgsbGdlieOr0
UwWuJCwzZuBDruMYAfyQBvYfXZun3Zm84rW7Jclp18mXITwGCVHg/P5n7QMbBfZQ
A25ymkuj636Nqh+c4zRnSINfyrDcID7AcqEb6IhJBBgRAgAJBQJJCfqnAhsMAAoJ
EBjAnoZeyUihPrcAniVWl5M44RuGctJe+IMNX4eVkC08AJ9v7cXsp5uDdQNo8q3R
8RHwN4Gk8w==
=3FTe
-----END PGP PUBLIC KEY BLOCK-----

It's also at
http://www.bitcoin.org/Satoshi_Nakamoto.asc

Email #244

Date: Tue, 07 Dec 2010 04:37:38 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: What was the bitcoin.org outage?

Attached is the root password encrypted.

> Thanks, did you finish moving bitcoinexchange to another server?

I moved all the files, database and bitcoind, but still some work
needed to get it running. The old site is down atm anyway, so feel
free to reboot if needed.

Email #245

Date: Tue, 07 Dec 2010 15:38:28 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Project Developers

To: Martti Malmi <mmalmi@cc.hut.fi>

Mind if I add you to the Project Developers list on the Contact page?
You wrote some code before so you should be there. It would have to be
your real name for consistency. If you want to have an e-mail address
listed, I'll make an image out of it so it doesn't attract spam.

Email #246

Date: Tue, 07 Dec 2010 18:12:58 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Project Developers

Ok. You can include the e-mail address.

> Mind if I add you to the Project Developers list on the Contact page?
> You wrote some code before so you should be there. It would have to be
> your real name for consistency. If you want to have an e-mail address

> listed, I'll make an image out of it so it doesn't attract spam.

Email #247

Date: Wed, 08 Dec 2010 23:09:45 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: [bitcoin-list] Bitcoin 0.3.18 is released

To: bitcoin-list@lists.sourceforge.net

Version 0.3.18 is now available.

Changes:
- Fixed a wallet.dat compatibility problem if you downgraded from 0.3.17 and then upgraded again
- IsStandard() check to only include known transaction types in blocks
- Jgarzik's optimisation to speed up the initial block download a little

The main addition in this release is the Accounts-based JSON-RPC commands that Gavin's been working on (more details at http://www.bitcoin.org/smf/index.php?topic=1886.0).
- getaccountaddress
- sendfrom
- move
- getbalance
- listtransactions

Download:
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.18/

---

bitcoin-list@lists.sourceforge.net
https://lists.sourceforge.net/lists/listinfo/bitcoin-list

Email #248

Date: Sat, 11 Dec 2010 20:36:32 +0200
From: mmalmi@cc.hut.fi
To: Gavin Andresen <gavinandresen@gmail.com>
Cc: satoshin@gmx.com
Subject: Resizing Bitcoin server

Bitcoin.org was down again today for some time. It responded to ping
but not ssh or http. I rebooted it and found out it was an out of
memory error and mysqld got killed. It was the same error last time,
but with apache getting killed. I couldn't think of anything better,
so I resized the server from 512MB to 1024MB of memory.

Email #249

Date: Mon, 13 Dec 2010 16:11:53 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: [bitcoin-list] Bitcoin 0.3.19 is released
To: bitcoin-list@lists.sourceforge.net

This is a minor release to add some DoS protection.

Changes:
- Added some DoS limits, though it's still far from DoS resistant.
- Removed "safe mode" alerts.

http://www.bitcoin.org/smf/index.php?topic=2228.0

Download:
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.19/

_____

bitcoin-list mailing list
bitcoin-list@lists.sourceforge.net
https://lists.sourceforge.net/lists/listinfo/bitcoin-list

Email #250

Date: Mon, 20 Dec 2010 17:55:04 +0200
From: mmalmi@cc.hut.fi
To: Gavin Andresen <gavinandresen@gmail.com>, Satoshi Nakamoto <satoshin@gmx.com>
Subject: Bitcoin.org backups

ShadowOfHarbringer described a way of mirroring the bitcoin.org website and forum here:
http://www.bitcoin.org/smf/index.php?topic=2026.msg30043#msg30043

Should we go by it and trust the database along with its password hashes to some reliable community members who have servers? Another option is to encrypt the backups with pgp and store them in multiple places.

Email #251

Date: Mon, 20 Dec 2010 18:10:06 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoin.org backups
To: Gavin Andresen <gavinandresen@gmail.com>
Cc: mmalmi@cc.hut.fi

Gavin Andresen wrote:
> On Mon, Dec 20, 2010 at 10:55 AM, <mmalmi@cc.hut.fi> wrote:
>> ShadowOfHarbringer described a way of mirroring the bitcoin.org website and
>> forum here:
>> http://www.bitcoin.org/smf/index.php?topic=2026.msg30043#msg30043
>>
>> Should we go by it and trust the database along with its password hashes to
>> some reliable community members who have servers?
>
> That seems like asking for trouble, and I think it would violate the
> implicit trust of everybody who's registered for the forums.

I agree, don't let the database out of your hands. There's private PM
in there, e-mail addresses, passwords.

BTW, password hashes = passwords. It's easy to break the hash of short
passwords people use on forums.
6 chars = 3 difficulty
7 chars = 410 difficulty
8 chars = 25418 difficulty

>> Another option is to
>> > encrypt the backups with pgp and store them in multiple places.
>
> That seems wiser. Daily backups copied ... somewhere ... seems like
> the right thing to do. If they're reasonably small (less than a
> gigabyte), I'd be happy to pay for Amazon S3 storage/bandwidth for
> them.

+1

Even with encryption, a trusted storage place is better.

Email #252

Date: Mon, 20 Dec 2010 23:21:27 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Cc: Gavin Andresen <gavinandresen@gmail.com>

Subject: Re: Bitcoin.org backups

Ok. I'll start backing up to another server I'm using. I'll send you
the SSH key when I've set it up, so you can start backing up to any
server you want. The backup file size is about 50 MB atm.

Here's my pgp key btw: http://www.bitcoin.org/mmalmi.asc

> Gavin Andresen wrote:
>> On Mon, Dec 20, 2010 at 10:55 AM, <mmalmi@cc.hut.fi> wrote:
>>> ShadowOfHarbringer described a way of mirroring the bitcoin.org website and
>>> forum here:
>>> http://www.bitcoin.org/smf/index.php?topic=2026.msg30043#msg30043

>>>
>>> Should we go by it and trust the database along with its password hashes to
>>> some reliable community members who have servers?
>>
>> That seems like asking for trouble, and I think it would violate the
>> implicit trust of everybody who's registered for the forums.
>
> I agree, don't let the database out of your hands. There's private PM
> in there, e-mail addresses, passwords.
>
> BTW, password hashes = passwords. It's easy to break the hash of short
> passwords people use on forums.
> 6 chars = 3 difficulty
> 7 chars = 410 difficulty
> 8 chars = 25418 difficulty
>
>
>>> Another option is to
>>>> encrypt the backups with pgp and store them in multiple places.
>>
>> That seems wiser. Daily backups copied ... somewhere ... seems like
>> the right thing to do. If they're reasonably small (less than a
>> gigabyte), I'd be happy to pay for Amazon S3 storage/bandwidth for
>> them.
>
> +1
>
> Even with encryption, a trusted storage place is better.

Email #253

Date: Tue, 21 Dec 2010 15:44:02 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Cc: Gavin Andresen <gavinandresen@gmail.com>

Subject: Re: Bitcoin.org backups

You can fetch the backup with:
wget --no-check-certificate
https://backup:cAr26Ram@www.bitcoin.org/backup/bitcoinsite.tar.bz2.gpg

It's updated every day 11:00 GMT.

Email #254

Date: Thu, 06 Jan 2011 18:31:26 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Writing about BitCoin

To: Gavin Andresen <gavinandresen@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

Gavin Andresen wrote:
> I'd be happy to talk to Rainey;

Great

> Satoshi, I assume you don't want to
> deal with press/PR/interviews ?

True

> We could decline to talk to the press-- Satoshi, I know you've
> expressed concern about bitcoin growing too big too fast, and being
> unable to keep up with traffic/attacks/feature requests/etc. But I
> don't think ignoring the press will make them go away; they'll just
> talk to somebody else. I think it is better to give a realistic
> impression of bitcoin (it is cutting-edge, beta software that is still
> being developed, it is not poised to replace PayPal or the Euro
> anytime soon, etc) rather than let somebody over-enthusiastic become
> "the unofficial bitcoin spokesperson."

You're the best person to do it.

EFF is really important. We want to have a good relationship with them.
  We're the type of project they like; they've helped the TOR project
and done a lot to protect P2P file sharing.

Email #255

Date: Tue, 25 Jan 2011 09:25:12 +0200

From: mmalmi@cc.hut.fi

To: satoshin@gmx.com

Subject: Fwd: Bitcoin question

Martti,
Thank you for the pdf. It looks great. I do not see a date on it. When was it written?

Mr. Mark Herpel of Digital Gold Currency Magazine brought Bitcoin to my attention for inclusion in my thesis. The thesis working title is: Digital Currency Systems: Emerging B2B e-Commerce Alternative During Monetary Crisis in the United States. I discuss the five types of systems per Mr. Herpels suggestion.

Appreciate it and hope to talk soon.

C.

Constance J. Wells, CeM, PMP: PMI certified
Denver, CO U.S.A.
303-730-6609

--- On **Mon, 1/24/11, mmalmi@cc.hut.fi <*mmalmi@cc.hut.fi*>** wrote:

> From: mmalmi@cc.hut.fi <mmalmi@cc.hut.fi>
> Subject: Re:
> To: "Constance J. Wells" <cjwells_1@yahoo.com>
> Date: Monday, January 24, 2011, 1:22 AM
>
> Hi Constance,
>
> Thanks for your interest in Bitcoin, feel free to cite. There's also Satoshi Nakamoto's paper available at http://www.bitcoin.org/bitcoin.pdf if you want something with a more formal touch. Please let us know when your thesis is finished!
>
> -Martti
>
> > Martti Malmi
> > Currently I am a full time student at-

> http://info.aspen.edu/
> Aspen University, in Denver, CO, 303-333-4224.
> Masters of Science in Technology and Innovation.
>
> I am writing my Thesis under the subject heading, digital currency systems. May I cite your site in my Thesis?
>
> Thank you.
> Constance
> Constance J. Wells, CeM, PMP: PMI certified
> Denver, CO U.S.A.
> 303-730-6609
>
>
>

Email #256

Date: Tue, 25 Jan 2011 18:34:03 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Fwd: Bitcoin question
To: mmalmi@cc.hut.fi

The paper was published in 2008.

Someone needs to correct Wikipedia; it incorrectly says the paper was published in 2009. The paper was released earlier than the software.

mmalmi@cc.hut.fi wrote:
> Can you comment on this?
>
> ----- Forwarded message from cjwells_1@yahoo.com -----
> Date: Mon, 24 Jan 2011 00:32:48 -0800 (PST)
> From: "Constance J. Wells" <cjwells_1@yahoo.com>

> Reply-To: "Constance J. Wells" <cjwells_1@yahoo.com>
> Subject: Re:
>   To: mmalmi@cc.hut.fi
>
> Martti,
> Thank you for the pdf. It looks great. I do not see a date on it. When
> was it written?
>
> Mr. Mark Herpel of Digital Gold Currency Magazine brought Bitcoin to my
> attention for inclusion in my thesis. The thesis working title is:
> Digital Currency Systems: Emerging B2B e-Commerce Alternative During
> Monetary Crisis in the United States. I discuss the five types of
> systems per Mr. Herpels suggestion.
>
> Appreciate it and hope to talk soon.
>
> C.
>
> Constance J. Wells, CeM, PMP: PMI certified
> Denver, CO   U.S.A.
> 303-730-6609
>
> --- On Mon, 1/24/11, mmalmi@cc.hut.fi <mmalmi@cc.hut.fi> wrote:
>
> From: mmalmi@cc.hut.fi <mmalmi@cc.hut.fi>
> Subject: Re:
> To: "Constance J. Wells" <cjwells_1@yahoo.com>
> Date: Monday, January 24, 2011, 1:22 AM
>
> Hi Constance,
>
> Thanks for your interest in Bitcoin, feel free to cite. There's also
> Satoshi Nakamoto's paper available at http://www.bitcoin.org/bitcoin.pdf
> if you want something with a more formal touch. Please let us know when
> your thesis is finished!
>
>
> -Martti
>
>> Martti Malmi
>> Currently I am a full time student at-
>> http://info.aspen.edu/
>> Aspen University, in Denver, CO, 303-333-4224.

>> Masters of Science in Technology and Innovation.
>>
>> I am writing my Thesis under the subject heading, digital currency
>> systems. May I cite your site in my Thesis?
>>
>> Thank you.
>> Constance
>> Constance J. Wells, CeM, PMP: PMI certified
>> Denver, CO U.S.A.
>> 303-730-6609
>>
>>
>>
>
>
>
>
>

Email #257

Date: Sun, 30 Jan 2011 21:01:53 +0200

From: mmalmi@cc.hut.fi

To: satoshin@gmx.com

Subject: Bookkeeping

+1781.28
-22.63 October hosting
-28.70 November hosting
-30.36 December hosting
-48.35 January hosting (server upscaled to 1024MB RAM)
+0.78 Annual interest on deposit

+1652.02

Since I'm no longer maintaining bitcoinexchange.com, I'm returning the 750€ to the project budget. I'll do this when I get a payment from the SMS gateway provider.

Email #258

Date: Mon, 07 Feb 2011 11:39:36 +0200

From: mmalmi@cc.hut.fi

Cc: "gavinandresen@gmail.com" <gavinandresen@gmail.com>, "satoshin@gmx.com" <satoshin@gmx.com>

Subject: Re: Bitcoin @ EPCA Conference Amsterdam 4-6 April?

Looks like an excellent opportunity to reach an important audience
that doesn't follow Slashdot or Reddit. I'd recommend this job for
Gavin or Bruce Wagner. Or maybe there can be two attendees. S3052 from
the forum also seemed potentially competent.

Gavin, would you be interested in organizing this?

> Hello,
>
> I am writing you on behalf of the EPCA Conference because we are
> interested to learn more about Bitcoin. Possibly Bitcoin is an
> interesting topic for the upcoming conference 4-6 April in Amsterdam.
>
> At this top rated conference we deal with the key strategic
> developments in the 'transaction industry' so not limited to
> payments. The event is truly 'professional for professional', so
> every presentation is screened on quality and relevance (no sales
> pitches). See also:
> www.epcaconference.com<http://www.epcaconference.com> .
>
> Since we discuss the most relevant topics in the industry, I would
> like to investigate whether the Bitcoin paradigm is interesting for
> the attendees. This should give the attendees (bankers and other
> financial professionals) a lot of inspiration for their own
> business. At the same time it is a good opportunity to position
> Bitcoin within the international audience, to gain unique strategic
> insights and to network within the European professional scene.
>
> Can we have contact this week to elaborate this further? Thank you
> in advance,
>
> Look forward hearing from you,
>
> Kind regards,
> Douwe Lycklama

> EPCA Conference Chaiman
>
>
>
> Douwe Lycklama | Innopay
> douwe@innopay.com<mailto:douwe@innopay.com>
> +31 655 711 150
>
> 'Imagine - Create - Innovate: Unlocking the Payments Potential'
> 10th international EPCA conference
> 4-6 April 2011, Amsterdam
> www.epcaconference.com<http://www.epcaconference.com/>
>
> Triport III 7th floor
> Westelijke Randweg 43
> 1118 CR SCHIPHOL AIRPORT
> The Netherlands
>
>

Email #259

Date: Thu, 10 Feb 2011 22:35:22 +0200
From: mmalmi@cc.hut.fi
To: Douwe Lycklama | Innopay <douwe@mail.innopay.com>
Cc: "gavinandresen@gmail.com" <gavinandresen@gmail.com>, "satoshin@gmx.com" <satoshin@gmx.com>
Subject: Re: Bitcoin @ EPCA Conference Amsterdam 4-6 April?

Hello,

Thanks for contacting and sorry for the late response. EPCA seems very interesting for the Bitcoin project, a good opportunity for networking. I'll find somebody who can work with you on this. In the meantime please ask me for any questions.

Best regards,

Martti Malmi
Bitcoin project developer

> Hello,
>
> I am writing you on behalf of the EPCA Conference because we are
> interested to learn more about Bitcoin. Possibly Bitcoin is an
> interesting topic for the upcoming conference 4-6 April in Amsterdam.
>
> At this top rated conference we deal with the key strategic
> developments in the 'transaction industry' so not limited to
> payments. The event is truly 'professional for professional', so
> every presentation is screened on quality and relevance (no sales
> pitches). See also:
> www.epcaconference.com<http://www.epcaconference.com> .
>
> Since we discuss the most relevant topics in the industry, I would
> like to investigate whether the Bitcoin paradigm is interesting for
> the attendees. This should give the attendees (bankers and other
> financial professionals) a lot of inspiration for their own
> business. At the same time it is a good opportunity to position
> Bitcoin within the international audience, to gain unique strategic
> insights and to network within the European professional scene.
>
> Can we have contact this week to elaborate this further? Thank you
> in advance,
>
> Look forward hearing from you,
>
> Kind regards,
> Douwe Lycklama
> EPCA Conference Chaiman
>
>
>
> Douwe Lycklama | Innopay
> douwe@innopay.com<mailto:douwe@innopay.com>
> +31 655 711 150
>
> 'Imagine - Create - Innovate: Unlocking the Payments Potential'
> 10th international EPCA conference
> 4-6 April 2011, Amsterdam
> www.epcaconference.com<http://www.epcaconference.com/>
>
> Triport III 7th floor

> Westelijke Randweg 43
> 1118 CR SCHIPHOL AIRPORT
> The Netherlands
>
>

Email #260

Date: Tue, 22 Feb 2011 19:49:19 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: 0.3.20 release : shipped

To: Gavin Andresen <gavinandresen@gmail.com>, Martti Malmi <mmalmi@cc.hut.fi>

> I have not sent a message to the sourceforge bitcoin-list mailing list
> because I don't think I have permission; Satoshi, can you give me
> permission, encrypt the mailman password with my public key and send
> it to me, or just post the announcement?

Martti should give you the Drupal admin password.

Any subscriber can post to bitcoin-list. Here's the admin password in
case you need it later.

Gavin:

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (MingW32) - WinPT 1.2.0

hQIOAxfAPINgyySWEAf9GHyuMqxkhoBe96hbHoFPIR4ORpMS/v2mpCT70UmgTt46
GVO5MeEOFE4JUqltYUaAE2u7e7+BbyNFeNk4o0kwJIWUXbRoBHj59vx+yzmeRLd9
YxTWxZA2zOVcYcYoDkiYAatwlQWQefzwYFcCnBSSsY1F9XLHMtLqNadhftOregoE
5Prhjk4ScAEOAmJ2CfYvWLD6FPAe4s6nXzP656oQghMgUivYoowHAjGUSvd8f1Qb
fkV0isGIYCpHCOSZDZpysPCm63ibEeiuylvkT7Ayj2HoonqypFdv05mtyS7Jtq6a
s06UqjLSyICoGJVk4x5HZhusgmbqViLvb6gM+iadbQf/U9KEKA5KyF0JvjYlx97k
Bm7WpBIxKnP6Migl/Otol85EYt9rWN0lozLGw5Ko1JTZzXv3RrTsJafUYnDyAvtR
20JExoG84LatTeFiTqVWHiWZbYG2ECJHTO6jOmITvNvq/OgCID4hQvjvNQiXghae
qzolzmZVEwDGAybWJoSvAsXjDWbAyHt9WJztHPgVRxgTBrnhoLAX0FwKGTCr7L/t
emVEUqgEf3WqmljD+cCXSNVloQxGmPvaSsbITIZvX/emwq4MAC+SuRmJLJp6kSmu
UhkxZMipvYHfyBPXoonAM7oYXNIaFQryS66UlEziSUevvU8TXiZMeUyyiMirOBXC
itKhAedpc7NQYG+/KohTS0U9QfdygBfE2o6M96tRKFdMmbQz3Gyq0BaBpp98+ve+
VOVp90mYv9zq43G7tHnZektEjGzplHj0HzWhfbiy2dBrDGhkByYN4G6kX0JvU4ZX

```
/ixmbOf5qZPqcgmz7fYDxKnkUQVumoEIfNXrUlAPcI2Ql9TnY0NIg9ZIVOGeT4lE
80kYloQVdCdnrJ7yLWexO0W1kSs=
=S7eV
-----END PGP MESSAGE-----

Martti:
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (MingW32) - WinPT 1.2.0

hQEMA+kEt/4bukJEAQgAlt5/Ks5pZPeusK0yefyMn7BqIVcOVHDaXbnf4dLKqq5J
6bKyMlkyYjhm1itZabi+IaV9k+1r7Wo50qOqfZNCSmG63hX3asXWd7QxThj4KDxr
fvuUfiduf2AyZcB4r/baw1hsdC3VGxQutU0ookuJqfvCIse77clS2WimKJ5hrh5G
KVdGApk3TxbILknalIs3mUw81sL0nvbO/aNrHiiNj44YU3Ehf5CieEJInHeYGTsJ
AABLZcH6B7nymA8D4nrAAnDcjcSE8+iWMOtzI2duCHKtA+LVJOsg8n/zHqK9SZNF
w+Xud7mBi/ZvnFGwCZh7cqJ/jZhNLLTQHiLr8M+i7dKhAekFho8aarOV9V4Cp2hT
a8bQdbgwsednyjCzaq+C8xU+aYJcAV95qK6QG2hlT8xpDU2KHBHWIjDmPKlzgvKb
8/dQo5VDvtQkdyvrd9pMJeOUxFKEVW5ph+4LzKjKEWE1kJhzAwbxQMNKkXLzZJIa
hJMNAVHDjnYcuI8EgJT+TjH2Kx+KwHX/OEOFaDXGP7XwMOuVZTVtbXnsJ24SFa1i
m4U=
=0TBL
-----END PGP MESSAGE-----
```

EXHIBIT B

ESSAYS

HOW TO MAKE A MINT: THE CRYPTOGRAPHY OF ANONYMOUS ELECTRONIC CASH*

LAURIE LAW
SUSAN SABETT
JERRY SOLINAS

TABLE OF CONTENTS

---

* This research Essay was prepared by NSA employees in furtherance of the study of cryptography. The contents of the report do not necessarily represent the position or policies of the U.S. Government, the Department of Defense, or the National Security Agency.

The authors are mathematical cryptographers at the National Security Agency's Office of Information Security Research and Technology.

INTRODUCTION

With the onset of the Information Age, our nation is becoming increasingly dependent on network communications. Computer-based technology is impacting significantly our ability to access, store, and distribute information. Among the most important uses of this technology is *electronic commerce*: performing financial transactions via electronic information exchanged over telecommunications lines. A key requirement for electronic commerce is the development of secure and efficient electronic payment systems. The need for security is highlighted by the rise of the Internet, which promises to be a leading medium for future electronic commerce.

Electronic payment systems come in many forms including digital checks, debit cards, credit cards, and stored value cards ("SVC"). The usual security features for such systems are privacy (protection from eavesdropping), authenticity (identification and message integrity), and nonrepudiation (prevention of later denying having performed a transaction).

This Essay focuses on electronic cash. As the name implies, electronic cash is an attempt to construct an electronic payment system modelled after our paper money system. Paper money has such features as: portability (easily carried); recognizability (as legal tender), and thus readily acceptable; transferability (without involvement of the financial network); untraceability (no record of where money is spent); anonymity (no record of who spent the money); and the ability to make "change." The designers of electronic cash focused on preserving the features of untraceability and anonymity. Thus, electronic cash is defined to be an electronic payment system that provides, in addition to the above security features, the properties of user anonymity and payment untraceability.

Electronic cash schemes that use digital signatures[1] to achieve

1. Editors' Note: For a thoughtful discussion of digital signatures, see Randy V. Sabett, *International Harmonization in Electronic Commerce and Electronic Data Interchange: A Proposed First*

security and anonymity are worrisome from a law enforcement perspective because of the anonymity feature. In particular, the dangers of money laundering and counterfeiting with electronic cash are potentially far more serious than with paper money. The widespread use of electronic cash would increase the vulnerability of the national financial system to "information warfare" attacks.[2] This Essay discusses measures to manage the risks associated with electronic cash; these safeguards, however, will have the effect of limiting user anonymity.

Part I defines the basic concepts surrounding electronic payment systems and electronic cash. Part II provides the reader with a high-level cryptographic description of electronic cash protocols in terms of basic authentication mechanisms. Part III describes specific existing implementations. The optional features of transferability and divisibility for off-line electronic cash are presented in Part IV. Part V discusses the security issues associated with electronic cash. Finally, this Essay concludes with a summary of the risks that are magnified by the presence of anonymity in electronic payment systems.

I. WHAT IS ELECTRONIC CASH?

The term "electronic cash" often is applied to any electronic payment scheme that superficially resembles money. In fact, however, electronic cash is a specific kind of electronic payment scheme, defined by certain cryptographic properties.

A. Electronic Payment

The term electronic commerce refers to any financial transaction involving the electronic transmission of information. The packets of information being transmitted commonly are called electronic tokens. One should not confuse the token, which is a sequence of bits, with the physical media used to store and transmit the information.

The storage medium generally is referred to as a "card" because it usually takes the form of a wallet-sized card made of plastic or cardboard. Two obvious examples are credit cards and ATM cards. However, the "card" also could be a computer memory.

An *electronic payment* is a particular kind of electronic commerce. An electronic payment protocol involves a series of transactions, resulting in a payment being made using a token issued by a third

---

Step Toward Signing on the Digital Dotted Line, 46 AM. U. L. REV. 511 (1996).

2. *See* CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 49 (Kenneth W. Dam & Herbert S. Lin eds., 1996).

party. The most common example is the electronic approval process used to complete a credit card transaction; neither payer nor payee issues the token in an electronic payment.[3]

The electronic payment scenario assumes three kinds of players:[4]

- a payer or consumer ("Alice"),
- a payee, such as a merchant ("Bob"), and
- a financial network with whom both Alice and Bob have accounts (the "Bank").

B. Security of Electronic Payments

With the rise of telecommunications and the Internet, it is increasingly common that electronic commerce takes place using a transmission medium not under the control of the financial system. It therefore is necessary to take steps to ensure the security of the messages sent along such a medium.

The necessary security properties are:

- *Privacy*, or protection against eavesdropping, which is important for transactions involving information such as credit card numbers sent on the Internet.
- *User identification*, or protection against impersonation.
- *Message integrity*, or protection against tampering or substitution, which ensures that the recipient's copy of the message is the same as what the sender sent.
- *Nonrepudiation*, or protection against later denial of a transaction.

The last three properties collectively are referred to as authenticity.

These security features can be achieved in several ways. One technique that is gaining widespread use is the establishment of an authentication infrastructure. In such a setup, privacy is attained by encrypting each message using a private key known only to the sender and the recipient. Authenticity is attained via key management, that is, the system of generating, distributing, and storing the users' keys.

Key management is carried out using a certification authority or a trusted agent who is responsible for confirming a user's identity. Certification is conducted for each user (including banks) who is issued a digital identity certificate. The certificate can be used whenever the user wishes to identify himself or herself to another user. Such certificates make it possible to set up a private key between users in a secure and authenticated way. The private key

3. In this sense, electronic payment differs from such systems as prepaid phone cards and subway fare cards, in which the token is issued by the payee.

4. Part IV.A generalizes this scenario in a discussion of transferability.

then is used to encrypt subsequent messages. This technique can be implemented to provide any or all of the above security features. Without a trusted certification authority and a secure authentication infrastructure, those security features cannot be achieved, and electronic commerce becomes impossible over an untrusted transmission medium.

The following discussion assumes that some authentication infrastructure is in place providing the four security features.

C. Electronic Cash

This Essay has defined privacy as protection against eavesdropping on one's communications. One privacy advocate, however, defines the term far more expansively.[5] To David Chaum, genuine "privacy" implies that one's history of purchases is not available for inspection by banks and credit card companies, and by extension, the government. To achieve this, one needs anonymity in addition to privacy. In particular, one needs (1) payer anonymity during payment; and (2) payment untraceability so that the bank cannot tell whose money is used in a particular payment.

These features are not available with credit cards. Indeed, the only conventional payment system offering these features is cash. Thus Chaum and others have introduced electronic cash (or digital cash) as an electronic payment system that offers both features.

The sequence of events in an electronic cash payment is as follows:

(1) withdrawal, in which Alice transfers some of her wealth from her Bank account to her card;
(2) payment, in which Alice transfers money from her card to Bob's; and
(3) deposit, in which Bob transfers the money he has received to his Bank account.

These procedures can be implemented in either of two ways:

- On-line payment means that Bob calls the Bank and verifies the validity of Alice's token[6] before accepting her payment and delivering his merchandise. This resembles many of today's credit card transactions.
- Off-line payment means that Bob submits Alice's electronic coin for verification and deposit sometime after the payment transaction is

5. *See generally* David Chaum, *Achieving Electronic Privacy*, SCI. AM., Aug. 1992, at 96; David Chaum, *Security Without Identification: Transactions to Make Big Brother Obsolete*, 28 ASS'N COMPUTING MACHINERY 1030 (1985).

6. In the context of electronic cash, the token usually is called an electronic coin.

completed. This method resembles making small purchases today by personal check.

Note that with an on-line system, the payment and deposit are not separate steps.

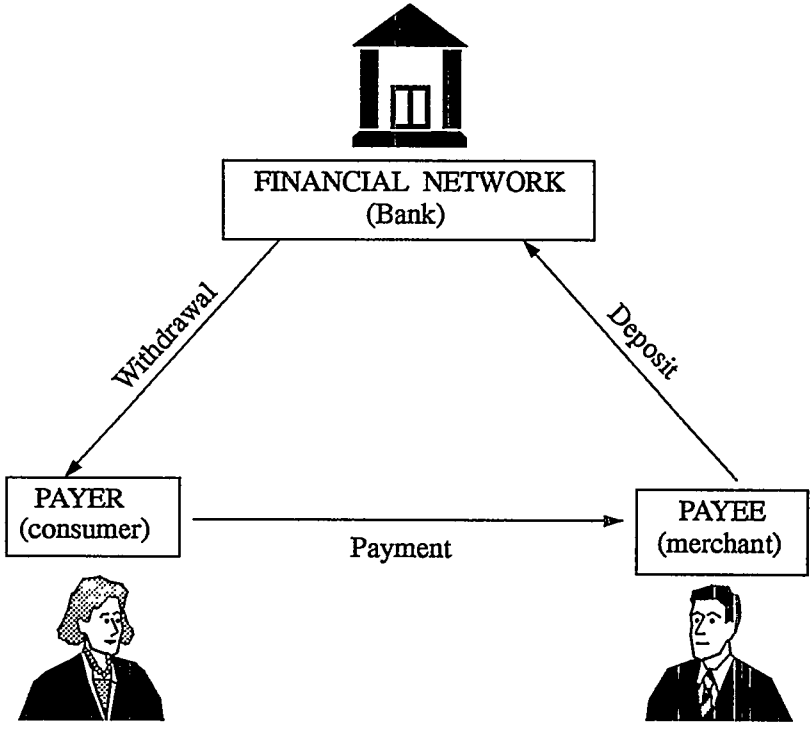


Figure 1. The three types of transactions in a basic electronic cash model.

D. Counterfeiting

As in any payment system, there is a potential for criminal abuse, with the intention either of cheating the financial system or of using the payment mechanism to facilitate some other crime. Part V will discuss criminal abuse further, but the issue of counterfeiting must be considered here, as the payment protocols contain built-in protections against it.

Two abuses of an electronic cash system are analogous to counterfeiting of physical cash:

- Token forgery, or creating a valid-looking coin without making a corresponding Bank withdrawal.
- Multiple spending, or using the same token over again. Because an electronic coin consists of digital information, it appears as valid after it has been spent as it did before.

Counterfeiting can be addressed by prevention or by detection after the fact in a way that identifies the culprit. Prevention clearly is preferable.

Although it is tempting to imagine electronic cash systems in which the transmission and storage media are secure, there certainly will be applications where this is not the case. An obvious example is the Internet, the users of which are notoriously vulnerable to viruses and eavesdropping. Thus, techniques other than physical security must be established to address counterfeiting.

- To protect against token forgery, one relies on the usual authenticity functions of user identification and message integrity. Note that the "user" being identified from the coin is the issuing Bank, not the anonymous spender.
- To protect against multiple spending, the Bank maintains a database of spent electronic coins. Coins already in the database are to be rejected for deposit. If the payments are on-line, this will prevent multiple spending. If the payments are off-line, detection of multiple spending is the only available precaution. To protect the payee, then, it is necessary to identify the payer. This means that the anonymity mechanism in the case of multiple spending must be disabled.

The features of authenticity, anonymity, and multiple-spender exposure are achieved most conveniently using public-key cryptography. Parts II and III will discuss how these features are accomplished using public key cryptography.

II. A CRYPTOGRAPHIC DESCRIPTION

Part II provides a high-level description of electronic cash protocols in terms of basic authentication mechanisms.

A. Public-Key Cryptographic Tools

Part A begins by discussing the basic public-key cryptographic techniques upon which the electronic cash implementations are based.

One-Way Functions. A one-way function is a correspondence between two sets that can be computed efficiently in one direction but not the other. In other words, the function ϕ is one-way if, given s in the domain of ϕ, it is easy to compute $t = \phi(s)$, but given only t, it is hard

to find *s*. (The elements are typically numbers, but also could be points on an elliptic curve, for example.[7])

Key Pairs. If ϕ is a one-way function, then a key pair is a pair *s*, *t* related in some way via ϕ. *s* is the secret key and *t* is the public key. As the names imply, each user keeps his secret key to himself and makes his public key available to all. The secret key remains secret even when the public key is known, because the one-way property of ϕ insures that *s* cannot be computed from *t*.

All public-key protocols use key pairs. For this reason, public-key cryptography often is called asymmetric cryptography, as opposed to conventional cryptography, which often is called symmetric cryptography, as one can both encrypt and decrypt with the private key but do neither without it.

Signature and Identification. In a public key system, a user identifies herself by proving that she knows her secret key without revealing it. She does this by performing some operation using the secret key that anyone can check or undo using the public key. This process is called identification. If one uses a message as well as one's secret key, one is performing a digital signature on the message. The digital signature plays the same role as a handwritten signature: identifying the author of the message in a way that cannot be repudiated and confirming the integrity of the message.

Secure Hashing. A hash function is a map from all possible strings of bits of any length to a bit string of fixed length. Such functions often are required to be collision-free: that is, it must be computationally difficult to find two inputs that hash to the same value. If a hash function is both one-way and collision-free, it is said to be a secure hash.

The most common use of secure hash functions is in digital signatures. Messages might come in any size, but a given public-key algorithm requires working in a set of fixed size. Thus one hashes the message and signs the secure hash rather than the message itself. The hash is required to be one-way to prevent signature forgery, that is, constructing a valid-looking signature of a message without using the secret key.[8] The hash must be collision-free to prevent repudiation, or denial of having signed one message by producing another message with the same hash.

---

7. *See* ALFRED J. MENEZES, ELLIPTIC CURVE PUBLIC KEY CRYPTOSYSTEMS 13 (1993).

8. Note that token forgery is not the same thing as signature forgery. Forging the Bank's digital signature without knowing its secret key is one way of committing token forgery, but not the only way. A bank employee or hacker, for instance, could "borrow" the Bank's secret key and validly sign a token. This key compromise scenario is discussed in Part V.C.

B. A Simplified Electronic Cash Protocol

The example below is a simplified electronic cash system protocol, without the anonymity features.

PROTOCOL 1: On-line electronic payment.
Withdrawal:
Alice sends withdrawal request to Bank.
Bank prepares electronic coin and digitally signs it.
Bank sends coin to Alice and debits her account.
Payment/Deposit:
Alice gives Bob coin.
Bob contacts Bank[9] and sends coin.
Bank verifies Bank's digital signature.
Bank verifies that coin has not already been spent.
Bank consults its withdrawal records to confirm Alice's withdrawal. (optional)
Bank enters coin in spent-coin database.
Bank credits Bob's account and informs Bob.
Bob gives Alice merchandise.

PROTOCOL 2: Off-line electronic payment.
Withdrawal:
Alice sends withdrawal request to Bank.
Bank prepares electronic coin and digitally signs it.
Bank sends coin to Alice and debits her account.
Payment:
Alice gives Bob coin.
Bob verifies Bank's digital signature. (optional)
Bob gives Alice merchandise.
Deposit:
Bob sends coin to Bank.
Bank verifies Bank's digital signature.
Bank verifies that coin has not already been spent.
Bank consults its withdrawal records to confirm Alice's withdrawal. (optional)
Bank enters coin in spent-coin database.

---

9. One should keep in mind that the term "Bank" refers to the financial system that issues and clears the coins. For example, the Bank might be a credit card company, or the overall banking system. In the latter case, Alice and Bob might have separate banks. If that is so, then the "deposit" procedure is slightly more complicated: Bob's bank contacts Alice's bank, "cashes in" the coin, and puts the money in Bob's account.

Bank credits Bob's account.

The above protocols use digital signatures to achieve authenticity. Although the authenticity features could have been achieved in other ways, digital signatures must be used to allow for the anonymity mechanisms to be added in the following discussion.

C. Untraceable Electronic Payments

In Part C, the above protocols are modified to include payment untraceability. To achieve untraceability, it is necessary that the Bank not be able to link a specific withdrawal with a specific deposit.[10] This is accomplished using a special kind of digital signature called a blind signature.

Examples of blind signatures are provided in Part III.B, but a high-level description is given here. In the withdrawal step, the user changes the message to be signed using a random quantity. This step is called "blinding" the coin, and the random quantity is called the blinding factor. The Bank signs this random-looking text, and the user removes the blinding factor. The user now has a legitimate electronic coin signed by the Bank. The Bank will see this coin when it is submitted for deposit, but will not know who withdrew it because the random blinding factors are unknown to the Bank. Obviously, it no longer will be possible to check the withdrawal records, which was an optional step in the first two protocols.

Note that the Bank does not know what it is signing in the withdrawal step. This introduces the possibility that the Bank might be signing something other than what it is intending to sign. To prevent this, a Bank's digital signature by a given secret key is valid only as authorizing a withdrawal of a fixed amount. For example, the Bank could have one key for a $10 withdrawal, another for a $50 withdrawal, and so on.[11]

PROTOCOL 3: Untraceable On-line electronic payment.
Withdrawal:

Alice creates electronic coin and blinds it.

Alice sends blinded coin to Bank with withdrawal request.

---

10. To achieve either anonymity feature, it is of course necessary that the pool of electronic coins be a large one.

11. One also could broaden the concept of "blind signature" to include interactive protocols in which both parties contribute random elements to the message to be signed. An example of this is the "randomized blind signature" occurring in the Ferguson scheme discussed in Part III.C.

Bank digitally signs blinded coin.
Bank sends signed blinded coin to Alice and debits her account.
Alice unblinds signed coin.

Payment/Deposit:

Alice gives Bob coin.
Bob contacts Bank and sends coin.
Bank verifies Bank's digital signature.
Bank verifies that coin has not already been spent.
Bank enters coin in spent-coin database.
Bank credits Bob's account and informs Bob.
Bob gives Alice merchandise.

PROTOCOL 4: Untraceable Off-line electronic payment.

Withdrawal:

Alice creates electronic coin and blinds it.
Alice sends blinded coin to Bank with withdrawal request.
Bank digitally signs blinded coin.
Bank sends signed blinded coin to Alice and debits her account.
Alice unblinds signed coin.

Payment:

Alice gives Bob coin.
Bob verifies Bank's digital signature. (optional)
Bob gives Alice merchandise.

Deposit:

Bob sends coin to Bank.
Bank verifies Bank's digital signature.
Bank verifies that coin has not already been spent.
Bank enters coin in spent-coin database.
Bank credits Bob's account.

D. A Basic Electronic Cash Protocol

Part D takes the final step in modifying the protocols to achieve payment anonymity. The ideal situation (from the point of view of privacy advocates) is that neither payer nor payee should know the identity of the other. This makes remote transactions using electronic cash completely anonymous: no one knows where Alice spends her money or who pays her.

Unfortunately, however, this level of anonymity is not possible: there is no way in such a scenario for the consumer to obtain a signed receipt. Thus, payer anonymity is all that can be achieved.

If the payment is to be on-line, Protocol 3, can be used (implemented, of course, to allow for payer anonymity). In the off-line case,

however, a new problem arises. If a merchant tries to deposit a previously spent coin, he will be turned down by the Bank, but neither will know who the multiple spender was, as she was anonymous. Thus, it is necessary for the Bank to be able to identify a multiple spender.

The solution is for the payment step to require the payer to have, in addition to her electronic coin, some sort of identifying information that she is to share with the payee. This information is split in such a way that any one piece reveals nothing about Alice's identity, but any two pieces are sufficient to identify her fully.

This information is created during the withdrawal step. The withdrawal protocol includes a step in which the Bank verifies that the information is present and corresponds to Alice and to the particular coin being created. To preserve payer anonymity, the Bank will not actually see the information, but only verify that it is there. Alice carries the information along with the coin until she spends it.

At the payment step, Alice must reveal one piece of this information to Bob. Thus only Alice can spend the coin, as only she knows the information. This revealing is done using a challenge-response protocol. In such a protocol, Bob sends Alice a random "challenge" quantity and, in response, Alice returns a piece of identifying information. The challenge quantity determines which piece she sends. At the deposit step, the revealed piece is sent to the Bank along with the coin. If all steps proceed properly, the identifying information never will point to Alice. Should she spend the coin twice, however, the Bank eventually will obtain two copies of the same coin, each with a piece of identifying information. Because of the randomness in the challenge-response protocol, these two pieces will be different. Thus the Bank will be able to identify her as the multiple spender. Because only Alice can dispense identifying information, it is clear that her coin was not copied and re-spent by someone else.

PROTOCOL 5: Off-line cash.
Withdrawal:
Alice creates electronic coin, including identifying information.
Alice blinds coin.
Alice sends blinded coin to Bank with withdrawal request.
Bank verifies that identifying information is present.
Bank digitally signs blinded coin.
Bank sends signed blinded coin to Alice and debits her account.
Alice unblinds signed coin.

Payment:
Alice gives Bob coin.
Bob verifies Bank's digital signature.
Bob sends Alice challenge.
Alice sends Bob response (revealing one piece of identifying information).
Bob verifies response.
Bob gives Alice merchandise.
Deposit:
Bob sends coin, challenge, and response to Bank.
Bank verifies Bank's digital signature.
Bank verifies that coin has not already been spent.
Bank enters coin, challenge, and response in spent-coin database.
Bank credits Bob's account.

Note that, in this protocol, Bob must verify the Bank's signature before giving Alice the merchandise. In this way, Bob can be sure that either he will be paid or he will learn Alice's identity as a multiple spender.

III. PROPOSED OFF-LINE IMPLEMENTATIONS

Having described electronic cash in a high-level format, this Essay now will describe the specific implementations that have been proposed. These implementations will be given for the off-line case only. The corresponding on-line protocols are just simplified versions of those provided below.

A. Including Identifying Information

Part A explains more specifically how to include (and access when necessary) the identifying information meant to catch multiple spenders. There are two ways to accomplish this task: the cut-and-choose method and zero-knowledge proofs.

Cut and Choose. When Alice wishes to make a withdrawal, she first constructs and blinds a message consisting of K pairs of numbers, where K is large enough that an event with probability 2^{-K} never will happen in practice. These numbers have the property of enabling one to identify Alice given both pieces of a pair; unmatched pieces remain useless. Alice then obtains signature of this blinded message from the Bank. This is done in such a way that the Bank can check that the K pairs of numbers are present and that they have the required properties despite the blinding.

When Alice spends her coins with Bob, his challenge to her is a string of K random bits. For each bit, Alice sends the appropriate

piece of the corresponding pair. For example, if the bit string starts *0110* . . ., Alice sends the first piece of the first pair, the second piece of the second pair, the second piece of the third pair, the first piece of the fourth pair, etc. When Bob deposits the coin at the Bank, he sends on these K pieces.

If Alice re-spends her coin, she is challenged a second time. Because each challenge is a random bit string, the new challenge is bound to disagree with the old one in at least one bit. Thus Alice will have to reveal the other piece of the corresponding pair. When the Bank receives the coin a second time, it takes the two pieces and combines them to reveal Alice's identity.

Although conceptually simple, this scheme is not very efficient, as each coin must be accompanied by $2K$ large numbers.

Zero-Knowledge Proofs. The term zero-knowledge proof refers to any protocol in public-key cryptography that proves knowledge of some quantity without revealing it or making it any easier to find. In this case, Alice creates a key pair such that the secret key points to her identity. This is done in such a way that the Bank can check via the public key that the secret key in fact reveals her identity, despite the blinding. In the payment protocol, Alice gives Bob the public key as part of the electronic coin. She then proves to Bob via a zero-knowledge proof that she possesses the corresponding secret key. If she responds to two distinct challenges, the identifying information can be put together to reveal the secret key and thus her identity.

B. Authentication and Signature Techniques

Part B describes the digital signatures that have been used in implementation of the above protocols and the techniques that have been used to include identifying information.

Two kinds of digital signatures appear in electronic cash protocols. Suppose the signer has a key pair and a message M to be signed.

- *Digital Signature with Message Recovery.* For this kind of signature, there is a signing function S_{SK} using the secret key SK, and a verifying function V_{PK} using the public key PK. These functions are inverses, so that:

  Equation 1: $$V_{PK}\,(S_{SK}\,(M)) = M.$$

  The function V_{PK} is easy to implement, but S_{SK} is easy only if one knows SK. Thus S_{SK} is said to have a trapdoor, or secret quantity that makes it possible to perform a cryptographic computation which is otherwise infeasible. The function V_{PK} is called a trapdoor one-way function, because it is a one-way function to anyone who does not know the trapdoor.

In this kind of scheme, the verifier receives the signed message $S_{SK}(M)$ but not the original message text. The verifier then applies the verification function V_{PK}. This step both verifies the identity of the signer and, by using Equation 1, recovers the message text.

- *Digital Signature with Appendix.* In this kind of signature, the signer performs an operation on the message using his own secret key. The result is taken to be the signature of the message, sent as an attached appendix to the message text. The verifier checks an equation involving the message, the appendix, and the signer's public key. If the equation checks, the verifier knows that the signer's secret key was used in generating the signature.

Specific algorithms are provided below.

RSA Signatures. The most well-known signature with message recovery is the RSA signature. Let N be a hard-to-factor integer. The secret signature key s and the public verification key v are exponents with the property that

$$M^{sv} \equiv M \pmod{N}$$

for all messages M. Given v, it is easy to find s if one knows the factors of N, but difficult otherwise. Thus the "v^{th} power (mod N)" map is a trapdoor one-way function. The signature of M is

$$C := M^s \pmod{N};$$

to recover the message (and verify the signature), one computes

$$M := C^v \pmod{N}.$$

Blind RSA Signatures. The above scheme is easily blinded. Suppose that Alice wants the Bank to produce a blind signature of the message M. She generates a random number r and sends

$$r^v M \pmod{N}$$

to the Bank to sign. The Bank does so, returning

$$r M^s \pmod{N}.$$

Alice then divides this result by r. The result is $M^s \pmod{N}$, the Bank's signature of M, even though the Bank never has seen M.

The Schnorr Algorithms. The Schnorr family of algorithms includes an identification procedure and a signature with appendix. These algorithms are based on a zero-knowledge proof of possession of a secret key. Let p and q be large prime numbers with q dividing $p - 1$. Let g be a generator; that is, an integer between 1 and p such that

$$g^q = 1 \pmod{p}.$$

If s is an integer (mod q), then the modular exponentiation operation on s is

$$\phi : \; s \geq g^s \pmod{p}.$$

The inverse operation is called the discrete logarithm function and is denoted

$$\log_g t \leq t.$$

If p and q are chosen properly, then modular exponentiation is a one-way function. That is, it is computationally infeasible to find a discrete logarithm. Now suppose we have a line:

Equation 2: $y = mx + b$

over the field of integers (mod q). A line can be described by giving its slope m and intercept b, but we will "hide" it as follows. Let

$$c = g^b \pmod{p},$$
$$n = g^m \pmod{p}.$$

Then c and n give us the "shadow" of the line under ϕ. Knowing c and n does not give the slope or intercept of the line, but it does enable us to determine whether a given point (x, y) is on the line. If (x, y) satisfies Equation 2, then it also must satisfy the relation below:

Equation 3 $g^y = n^x \, c \pmod{p}.$

Conversely, any point (x, y) satisfying Equation 3 must be on the line. The relationship in Equation 3 can be checked by anyone, because it involves only public quantities. Thus anyone can check whether a given point is on the line, but points on the line can be generated only by someone who knows the secret information. The basic Schnorr protocol is a zero-knowledge proof that one possesses a given secret quantity m. Let n be the corresponding public quantity. Suppose one user (the "prover") wants to convince another (the "verifier") that she knows m without revealing it. She does this by constructing a line (Equation 2) and sending its shadow to the verifier. The slope of the line is taken to be secret quantity m, and the prover chooses the intercept at random, differently for each execution of the protocol. The protocol then proceeds as follows:

Schnorr proof of possession:

(1) Alice sends c (and n if necessary) to Bob.

(2) Bob sends Alice a "challenge" value of x.

(3) Alice responds with the value of y such that (x, y) is on the line.

(4) Bob verifies via Equation 3 that (x, y) is on the line.

Bob now knows that he is speaking with someone who can generate points on the line. Thus Alice must know the slope of the line, which is the secret quantity m.

An important feature of this protocol is that it can be performed only once per line. For example, if Bob knows any two points (x_0, y_0) and (x_1, y_1) on the line, he can compute the slope of the line using the familiar "rise over run" formula

$$m \equiv (y_0 - y_1) \,/\, (x_0 - x_1) \pmod{q},$$

and this slope is the secret quantity m. That is why a new intercept must be generated each time a message is sent. This is known as the *two-points-on-a-line principle.* This feature will be useful for electronic cash protocols, because we want to define a spending procedure that reveals nothing of a secret key if used once per coin, but reveals the key if a coin is spent twice.

Schnorr identification. The above protocol can be used for identification of users in a network. Each user is issued a key pair, and each public key is advertised as belonging to a given user. To identify herself, a user need prove only that she knows her secret key. This can be accomplished using the above zero-knowledge proof, because her public key is linked with her identity.

Schnorr Signature. It is easy to convert the Schnorr identification protocol to produce a digital signature scheme. Rather than receiving a challenge from an on-line verifier, the signer simply takes x to be a secure hash of the message and of the shadow of the line. This proves knowledge of his secret key in a way that links his key pair to the message.

Blind Schnorr Signature. Suppose that Alice wants to obtain a blind Schnorr signature for her coin, which she will spend with Bob. Alice generates random quantities (mod q) which describe a change of variables. This change of variables replaces the Bank's hidden line with another line, and the point on the Bank's line with a point on the new line. When Bob verifies the Bank's signature, he is checking the new point on the new line. The two lines have the same slope, so that the Bank's signature will remain valid. When the Bank receives the coin for deposit, it will see the protocol implemented on the new line, but it will not be able to link the coin with Alice's withdrawal because only Alice knows the change of variables relating the two lines.

Chaum-Pedersen Signature. A variant of Schnorr's signature scheme is used in electronic cash protocols.[12] This modified scheme is a kind of "double Schnorr" scheme. It involves a single line and point but uses two shadows. This signature scheme can be blinded in a way similar to the ordinary Schnorr signature.

Implementations of the Schnorr Protocols. The Schnorr algorithms have been described in terms of integers modulo a prime p. The protocols, however, work in any setting in which the analogue of the discrete logarithm problem is difficult. An important example is that of elliptic curves.[13] Elliptic curve based protocols are much faster and require the transmission of far less data than non-elliptic protocols giving the same level of security.

C. *Summary of Proposed Implementations*

Part C presents summaries of the three main off-line cash schemes: Chaum-Fiat-Naor,[14] Brands,[15] and Ferguson.[16]

Chaum-Fiat-Naor was the first electronic cash scheme, and is the simplest conceptually. The Bank creates an electronic coin by performing a blind RSA signature to Alice's withdrawal request, after verifying interactively that Alice has included her identifying information on the coin. The prevention of multiple spending is accomplished by the cut-and-choose method. For this reason, the scheme is relatively inefficient.

Brands' scheme is Schnorr-based.[17] Indeed, a Schnorr protocol is used twice: at withdrawal the Bank performs a blind Chaum-Pedersen signature, and then Alice performs a Schnorr possession proof as the challenge-and-response part of the spending protocol.

The withdrawal step produces a coin that contains the Bank's signature, authenticating both Alice's identifying information and the shadow of the line to be used for the possession proof. This commits Alice to using that particular line in the spending step. If she respends the coin, she must use the same line twice, enabling the Bank to identify her.

---

12. *See* David Chaum & Torben P. Pedersen, *Wallet Databases With Observers*, 1992 ADVANCES IN CRYPTOLOGY—CRYPTO '92, LECTURE NOTES IN COMPUTER SCI. 89, 93-94.

13. *See* MENEZES, *supra* note 7, at 13.

14. *See* David Chaum et al., *Untraceable Electronic Cash*, 1988 ADVANCES IN CRYPTOLOGY—CRYPTO '88, LECTURE NOTES IN COMPUTER SCI. 319.

15. *See* Stefan Brands, *Untraceable Off-line Cash in Wallets with Observers*, 1993 ADVANCES IN CRYPTOLOGY—CRYPTO '93, LECTURE NOTES IN COMPUTER SCI. 302.

16. *See* Niels Ferguson, *Single Term Off-line Coins*, 1993 ADVANCES IN CRYPTOLOGY—EUROCRYPT '93, LECTURE NOTES IN COMPUTER SCI. 318.

17. For ease of exposition, we give a simplified account of Brands' protocol.

The Brands scheme is considered by many to be the best of the three, for two reasons: (1) it avoids the awkward cut-and-choose technique; and (2) it is based only on the Schnorr protocols, and this can be implemented in various settings such as elliptic curves.

Ferguson's scheme is RSA-based like Chaum-Fiat-Naor, but it uses the "two-points-on-a-line" principle like Brands. The signature it uses is not the blind RSA signature as described above, but a variant called a randomized blind RSA signature. The ordinary blind RSA scheme has the drawback that the Bank has absolutely no idea what it is signing. As mentioned above, this is not a problem in the cut-and-choose case, but in this case it can allow a payer to defeat the mechanism for identifying multiple spenders. The randomized version avoids this problem by having both Alice and the Bank contribute random data to the message. The Bank still does not know what it is signing, but it knows that the data was not chosen maliciously. The rest of the protocol is conceptually similar to Brands' scheme. The message to be signed by the Bank contains, in addition to the random data, the shadow of a line the slope and intercept of which reveal Alice's identity. During payment, Alice reveals a point on this line; if she does so twice, the Bank can identify her. Although Ferguson's scheme avoids the cut-and-choose technique, it is the most complicated of the three (due largely to the randomized blind RSA signature). Moreover, it cannot be implemented over elliptic curves because it is RSA-based.

IV. OPTIONAL FEATURES OF OFF-LINE CASH

Part IV discusses two features that can be added to off-line cash to make it more convenient to use.

A. Transferability

Transferability is a feature of paper cash that allows a user to spend a coin that he has received in a payment without having to contact the Bank first. A payment is referred to as a transfer if the payee can use the received coin in a subsequent payment. A payment system is transferable if it allows at least one transfer per coin. Figure 2 shows a maximum length path of a coin in a system that allows two transfers. The final payment is not considered a transfer because it must be deposited by the payee. Transferability would be a convenient feature for an off-line cash system because it requires less interaction with the Bank. It should be noted that a transferable electronic cash system is off-line by definition, as on-line systems require communication with the Bank during each payment.

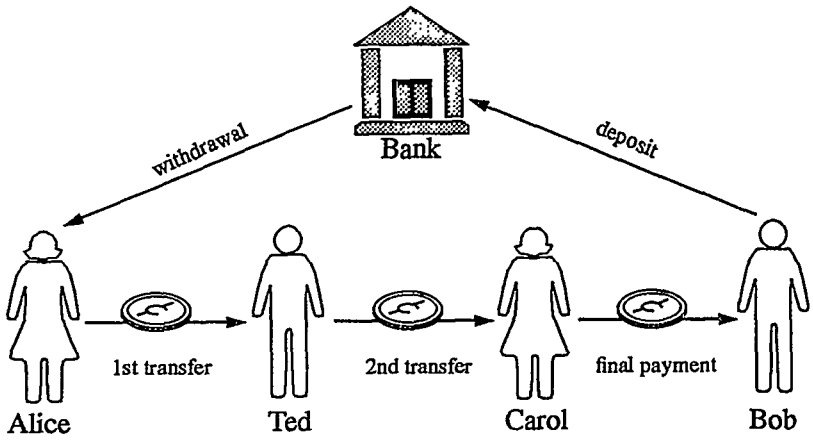


Figure 2. A maximum length path of a coin in a system which allows 2 transfers per coin.

Transferable systems have received little attention in academic literature. The schemes presented in Part III.C are not transferable because the payee cannot use a received coin in another payment; his only options are to deposit or exchange it for new coins at the Bank. Any transferable electronic cash system has the property that the coin must "grow in size" (i.e., accumulate more bits) each time it is spent, because the coin must contain information about every person who has spent it so that the Bank maintains the ability to identify multiple spenders.[18] This growth makes it impossible to allow an unlimited number of transfers. The maximum number of transfers allowed in any given system will be limited by the allowable size of the coin.

Other concerns with any transferable electronic cash system exist, even if the number of transfers per coin is limited, and the anonymity property is removed. Until the coin is deposited, the only information available to the Bank is the identity of the individual who originally withdrew the coin. Any other transactions involving that withdrawal can be reconstructed only with the cooperation of each consecutive spender of that coin. This poses the same problems that paper cash poses for detecting money laundering and tax evasion: no records of the transactions are available.

18. *See generally* David Chaum & Torben P. Pedersen, *Transferred Cash Grows in Size*, 1992 ADVANCES IN CRYPTOLOGY—EUROCRYPT '92, LECTURE NOTES IN COMPUTER SCI. 390.

In addition, each transfer delays detection of re-spent or forged coins. Multiple spending will not be noticed until two copies of the same coin eventually are deposited. By then it may be too late to catch the culprit, and many users may have accepted counterfeit coins. Detection of multiple spending after the fact, therefore, may not provide a satisfactory solution for a transferable electronic cash system. Rather, a transferable system may have to rely on physical security to prevent multiple spending.[19]

B. Divisibility

Suppose that Alice is enrolled in a non-transferable, off-line cash system, and she wants to purchase an item from Bob that costs $4.99. If she happens to have electronic coins the value of which adds up to exactly $4.99 then she simply spends these coins. Unless Alice has stored a large reserve of coins of each possible denomination, however, it is unlikely that she will have the exact change for most purchases. She may not wish to keep such a large reserve of coins on hand for some of the same reasons an individual does not carry around a large amount of cash: loss of interest and fear of the cash being stolen or lost. Another option is for Alice to withdraw a coin of the exact amount for each payment, but that requires interaction with the Bank, making the payment on-line from her point of view. A third option is for Bob to pay Alice the difference between her payment and the $4.99 purchase price. This puts the burden of having an exact payment on Bob, and also requires Alice to contact the Bank to deposit the "change."

A solution to Alice's dilemma is to use divisible coins: coins that can be "divided" into pieces the total value of which is equal to the value of the original coin. This allows exact off-line payments to be made without the need to store a supply of coins of different denominations. Paper cash obviously is not divisible, but lack of divisibility is not as much of an inconvenience with paper cash because it is transferable. Coins that are received in one payment can be used again in the next payment, so the supply of different denominations is partially replenished with each transaction.

Three divisible off-line cash schemes have been proposed, but at the cost of longer transaction time and additional storage. Eng/Okamoto's divisible scheme is based on the "cut and choose"

19. *See infra* Part V.A.

method.[20] Okamoto's scheme is much more efficient and is based on Brands' scheme but also will work on Ferguson's scheme.[21] Okamoto and Ohta's scheme is the most efficient of the three, but also the most complicated.[22] It relies on the difficulty of factoring and on the difficulty of computing discrete logarithms.

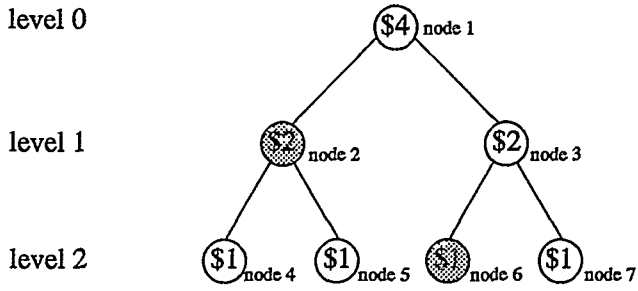


Figure 3. A binary tree for a divisible coin worth $4.00, with a minimum unit of $1.00. A $3.00 payment can be made by spending the shaded nodes. Node 1 cannot be used in a subsequent payment because it is an ancestor of nodes 2 and 6. Nodes 4 and 5 cannot be used because they are descendants of node 2. Node 3 cannot be used because it is an ancestor of node 6. Nodes 2 and 6 cannot be used more than once, so node 7 is the only node which can be spent in a subsequent payment.

All three of these schemes work by associating a binary tree with each coin of value $\$w$. Each node is assigned a monetary value as follows: the unique *root* node (the node at level 0) has value $\$w$, the two nodes at level 1 each have value $\$w/2$, the four nodes at level 2 each have value $\$w/4$, etc. Therefore, if $w = 2^l$, then the tree has $l+1$ levels, and the nodes at level j each have value $\$w/2^j$. The *leaves* of the tree are the nodes at level l, and have the minimum unit of value.

To spend the entire amount of value $\$w$, the root node is used. Amounts less than $\$w$ can be spent by spending a set of nodes the values of which add up to the desired amount.

Initially, any whole dollar amount up to $\$w$ can be spent. Subsequent payments are made according to the following rules:

---

20. *See* Tony Eng & Tatsuaki Okamoto, *Single-Term Divisible Electronic Coins*, 1994 ADVANCES IN CRYPTOLOGY—EUROCRYPT '94, LECTURE NOTES IN COMPUTER SCI. 311, 313.

21. *See generally* Tatsuaki Okamoto, *An Efficient Divisible Electronic Cash Scheme*, 1995 ADVANCES IN CRYPTOLOGY—CRYPTO '95, LECTURE NOTES IN COMPUTER SCI. 438.

22. *See generally* Tatsuaki Okamoto & Kazuo Ohta, *Universal Electronic Cash*, 1991 ADVANCES IN CRYPTOLOGY—CRYPTO '91, LECTURE NOTES IN COMPUTER SCI. 324.

(1) Once a node is used, none of its descendant and ancestor nodes[23] can be used; and

(2) No node can be used more than once.

These two rules ensure that no more than one node is used on any path from the root to a leaf. If these two rules are observed, then it will be impossible to spend more than the original value of the coin. If either of these rules are broken, then two nodes on the same path are used, and the information in the two corresponding payments can be combined to reveal the identity of the individual who over-spent in the same way that the identity of a multiple spender is revealed.

More specifically, in the Eng/Okamoto and Okamoto schemes, each user has a secret value s, which is linked to his identity. Uncovering s will uncover the user's identity, but not vice-versa. Each node i is assigned a secret value, t_i. Thus, each node i corresponds to a line

$$y = sx + t_i .$$

When a payment is made using a particular node n, t_i will be revealed for all nodes i that are ancestors of node n. The payee then sends a challenge x_1 and the payer responds with

$$y_1 = sx_1 + t_n .$$

This reveals a point (x_1, y_1) on the line $y = sx + t_n$, but does not reveal the line itself. If the same node is spent twice, then responses to two independent challenges, x_1 and x_2, will reveal two points on the same line: (x_1, y_1) and (x_2, y_2). The secret value s can be recovered using the two-points-on-a-line principle described in Part III.B.

If someone tries to overspend a coin, then two nodes in the same path will be used. Suppose that nodes n and m are in the same path, and node n is farther from the root on this path. Spending node n will reveal t_m, because node m is an ancestor of node n. If node m also is spent, then the response to a challenge x_1 will be $y_1 = sx_1 + t_m$. But t_m was revealed when t_n was spent, so sx_1 and hence s will be revealed. Therefore, spending two nodes in the same path will reveal the identity of the over-spender. The Okamoto/Ohta divisible scheme also uses a binary tree with the same rules for using nodes to prevent multiple and over-spending, but when nodes are used improperly, a different technique is used to determine the identity of the spender. Instead of hiding the user's identifying secret in a line

23. A descendant of a node n is a node on a path from node n to a leaf. An ancestor of node n is a node on the path from node n to the root node.

for which a point is revealed when a coin is spent, the user's identifying secret is hidden in the factorization of an RSA modulus. Spending the same node twice, or spending two nodes on the same path will provide enough information for the Bank to factor the modulus (which is part of the coin) and then to compute the user's secret identifying information.

Although these three divisible schemes are untraceable, payments made from the same initial coin may be "linked" to each other, meaning that it is possible to tell if two payments came from the same coin and thus the same person. This does not reveal the payer's identity if both payments are valid (following Rules 1 and 2, *supra*), but revealing the payer's identity for one purchase would reveal that payer's identity for all other purchases made from the same initial coin.

Although providing divisibility complicates the protocol, it can be accomplished without forfeiting untraceability or the ability to detect improper spenders using any of these schemes. The most efficient divisible scheme has a transaction time and required memory per coin proportional to the logarithm of N, where N is the total coin value divided by the value of the minimum divisible unit. More improvements in the efficiency of divisible schemes are expected, as the most recent improvement was presented in 1995.

V. SECURITY ISSUES

Part V discusses some issues concerning the security of electronic cash. First, Parts A and B discuss ways to prevent multiple spending in off-line systems and describe the concept of wallet observers. Part C discusses the consequences of an unexpected failure in the system's security. Finally, Part D describes a solution to some of the law enforcement problems that are created by anonymity.

A. Multiple Spending Prevention

Part I.D explained that multiple spending can be prevented in on-line payments by maintaining a database of spent electronic coins, but there is no cryptographic method for preventing an off-line coin from being spent more than once. Instead, off-line multiple spending is detected when the coin is deposited and compared to a database of spent coins. Even in anonymous, untraceable payment schemes, the identity of the multiple-spender can be revealed when the abuse is detected. Detection after the fact may be enough to discourage multiple spending in most cases, but it will not solve the problem. If someone were able to obtain an account under a false identity, or

were willing to disappear after re-spending a large sum of money, he could cheat the system successfully.

One way to minimize the problem of multiple spending in an off-line system is to set an upper limit on the value of each payment. This would limit the financial losses to a given merchant from accepting coins that had been deposited previously. However, this will not prevent someone from spending the same small coin many times in different places.

In order to prevent multiple spending in off-line payments, one must rely on physical security. A "tamper-proof" card could prevent multiple spending by removing or disabling a coin once it is spent. Unfortunately, a truly "tamper-proof" card does not exist. Instead, we will refer to a "tamper-resistant" card that physically is constructed so that it is very difficult to modify its contents. This could be in the form of a smart card, a PCMCIA card, or any storage device containing a tamper-resistant computer chip. A tamper-resistant card will prevent abuse in most cases, because the typical criminal will not have the resources to modify the card. Even with a tamper-resistant card, however, it still is essential to provide cryptographic security to prevent counterfeiting and to detect and identify multiple spenders if the tamper-protection somehow is defeated. Additionally, setting limits on the value of off-line payments would reduce the cost-effectiveness of tampering with the card.

Tamper-resistant cards also can provide personal security and privacy to the cardholder by making it difficult for adversaries to read or modify the information stored on the card, such as secret keys, algorithms, or records.

B. Wallet Observers

All of the basic off-line cash schemes presented in Part III.C can cryptographically detect the identity of multiple spenders, but the only way to prevent off-line multiple spending is to use a tamper-resistant device such as a smart card. One drawback of this approach is that the user must put a great deal of trust in the device, because the user loses the ability to monitor information entering or leaving the card. It is conceivable that the tamper-resistant device could leak private information about the user without the user's knowledge.

Chaum and Pedersen proposed the idea of embedding a tamper-resistant device into a user-controlled outer module in order to achieve the security benefits of a tamper-resistant device without

requiring the user to trust the device.[24] They call this combination an electronic wallet. The outer module (such as a small hand-held computer or the user's PC) is accessible to the user. The inner module, which cannot be read or modified, is called the "observer." All information that enters or leaves the observer must pass through the outer module, allowing the user to monitor information that enters or leaves the card. The outer module, however, cannot complete a transaction without the cooperation of the observer. This gives the observer the power to prevent the user from making transactions that it does not approve of, such as spending the same coin more than once.

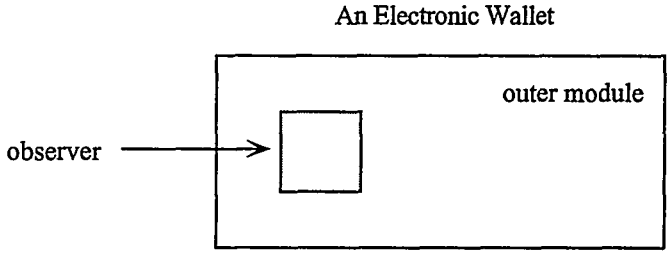


Figure 4. An electronic wallet.

Brands and Ferguson both have shown how to incorporate observers into their respective electronic cash schemes to prevent multiple spending.[25] Brands' scheme incorporates observers in a much simpler and more efficient manner. In Brands' basic scheme, the user's secret key is incorporated into each of his coins. When a coin is spent, the spender uses his secret key to create a valid response to a challenge from the payee. The payee will verify the response before accepting the payment. Using Brands' scheme with wallet observers, this user-secret key is shared between the user and his observer. The combined secret is a modular sum of the two shares, so that one share of the secret reveals no information about the combined secret. Cooperation of the user and the observer is necessary to create a valid response to a challenge during a payment transaction. This is accomplished without either the user or the observer revealing any information about its share of the secret to the

24. *See* Chaum & Pedersen, *supra* note 12, at 92-93.

25. *See generally* Brands, *supra* note 15; Niels Ferguson, *Extensions of Single-term Coins*, 1993 ADVANCES IN CRYPTOLOGY, LECTURE NOTES IN COMPUTER SCI. 292.

other. It also prevents the observer from controlling the response; thus the observer cannot leak any information about the spender.

An observer also could be used to trace the user's transactions at a later time, as it can keep a record of all transactions in which it participates. However, this requires that the Bank (or whoever is doing the tracing) be able to obtain the observer and analyze it. Also, not all types of observers can be used to trace transactions. Brands and Ferguson both claim that they can incorporate observers into their schemes and still retain untraceability of the users' transactions, even if the observer used in the transactions has been obtained and can be analyzed.

C. Security Failures

1. Types of failures

In any cryptographic system, there is some risk of a security failure. Such a failure in an electronic cash system would result in the ability to forge or duplicate money. There are a number of different ways in which an electronic cash system could fail.

One of the most serious types of failure would occur if the cryptography (the protocol or the underlying mathematics) does not provide the intended security.[26] This could enable someone to create valid looking coins without knowledge of an authorized bank's secret key, or to obtain valid secret keys without physical access to them. Anyone who is aware of the weakness could create coins that appear to come from a legitimate bank in the system.

Another serious type of failure could occur in a specific implementation of the system. For example, if the bank's random number generator is not a good one, an individual may be able to guess the secret random number and use it to compute the secret keys that are used to create electronic money.

Even if the cryptography and the implementation are secure, the security could fail because of a physical compromise. If a computer hacker, a thief, a dishonest bank employee, or a rogue state were to gain access to the bank's secret key it could create counterfeit money. If it gains access to a user's secret key it could spend that user's money. If it modifies the user or bank's software they could destroy the security of the system.

---

26. The authors are unaware of anything in the literature that would suggest this type of failure with the protocols discussed in this Essay.

The above failure scenarios apply not only to the electronic cash system, but also to the underlying authentication infrastructure. Any form of electronic commerce depends heavily on the ability of users to trust the authentication mechanisms. If, for example, an attacker could demonstrate a forgery of the certification authority's digital signature, it would undermine the users' trust in the ability of the parties to identify each other. Thus, certification authorities must secured as thoroughly as banks.

2. Consequences of a failure

All three of the basic schemes described in this Essay are anonymous, which makes it impossible for anyone to connect a deposited coin to the originating bank's withdrawal record of that coin. This property has serious consequences in the event of a security failure leading to token forgery. When a coin is submitted for deposit, it is impossible to determine if it is forged. Even the originating bank is unable to recognize its own coins, preventing detection of the compromise. It is conceivable that the compromise will not be detected until the bank realizes that the total value of deposits of its electronic cash exceeds the amount that it has created with a particular key. At this point the losses could be devastating.

After the key compromise is discovered, the bank still will be unable to distinguish valid coins from invalid ones, as deposits and withdrawals cannot be linked. The bank would have to change its secret key and invalidate all coins that were signed with the compromised key. The bank can replace coins that have not been spent yet, but the validity of untraceable coins that already have been spent or deposited cannot be determined without cooperation of the payer. Payment untraceability prevents the Bank from determining the identity of the payer, and payer anonymity prevents even the payee from identifying the payer.

It is possible to minimize this damage by limiting the number of coins affected by a single compromise. This could be done by changing the Bank's public key at designated time intervals, or when the total value of coins issued by a single key exceeds a designated limit. This kind of compartmentation, however, reduces the anonymity by shrinking the pool of withdrawals that could correspond to a particular deposit and vice versa.

D. Restoring Traceability

The anonymity properties of electronic cash pose several law enforcement problems because they prevent withdrawals and deposits

from being linked to each other. Part C explained how this linking problem prevents detection of forged coins. Anonymity also makes it difficult to detect money laundering and tax evasion because there is no way to link the payer and payee. Finally, electronic cash paves the way for new versions of old crimes such as kidnapping and blackmail[27] where money drops now can be carried out safely from the criminal's home computer.[28]

One way to minimize these concerns is to require large transactions or large numbers of transactions in a given time period to be traceable. This would make it more difficult to commit crimes involving large sums of cash. Even a strict limit such as a maximum of $100 a day on withdrawals and deposits can add up quickly, however, especially if one can open several accounts, each with its own limit. Also, limiting the amount spent in a given time period would have to rely on a tamper-resistant device.

Another way to minimize these concerns is to provide a mechanism to restore traceability under certain conditions, such as a court order. Traceability can be separated into two types by its direction. Forward traceability is the ability to identify a deposit record (and thus the payee), given a withdrawal record (and thus the identity of the payer). In other words, if a search warrant is obtained for Alice, forward tracing will reveal where Alice has spent her cash. Backward traceability is the ability to identify a withdrawal record (and thus the payer), given a deposit record (and thus the identity of the payee). Backward tracing will reveal who Alice has been receiving payments from.

A solution that conditionally restores both forward and backward traceability into the cut-and-choose scheme is presented by Stadler, Piveteau, and Camenisch.[29] In the basic cut-and-choose scheme, an identifying number is associated with each withdrawal record and a different identifying number is associated with each deposit record, although there is no way to link these two records to each other. To provide a mechanism for restoring backward traceability, the withdrawal number (along with some other data that cannot be associated with the withdrawal) is encrypted with a commonly trusted entity's public key and incorporated into the coin itself. This

---

27. *See* Sebastiaan von Solms & David Naccache, *On Blind Signatures and Perfect Crimes*, 11 COMPUTERS & SECURITY 581, 582-83 (1992).

28. This Essay does not focus on such crimes against individuals, concentrating instead on crimes against the government, the banking system, and the national economy.

29. *See generally* Markus Stradler et al., *Fair Blind Signatures*, 1995 ADVANCES IN CRYPTOLOGY—EUROCRYPT '95, LECTURE NOTES IN COMPUTER SCI. 209.

encrypted withdrawal number is passed to the payee as part of the payment protocol, and then passed along to the bank when the coin is deposited by the payee. The payer performs the encryption during the withdrawal transaction, but the bank can insure that the encryption was done properly. If the required conditions for tracing are met, the payment or deposit can be turned over to the trusted entity holding the secret key to decrypt the withdrawal number. This withdrawal number will allow the bank to access its withdrawal records, identifying the payer.

To provide a mechanism for restoring forward traceability, the payer must commit to a deposit number at the time that the coin is withdrawn. The payer encrypts this deposit number with a commonly trusted entity's public key (along with some other data that cannot be associated with the deposit) and must send this value to the bank as part of the withdrawal protocol. The bank is able to determine that the payer has not cheated, although it only sees the deposit number in encrypted form. If the required conditions for tracing are met, the withdrawal record can be turned over to the trusted entity holding the secret key to decrypt the deposit number. The bank can use this deposit number to identify the depositor (the payee).

Stadler, Piveteau, and Camenisch have shown that it is possible to provide a mechanism for restoring traceability in either or both directions. This can be used to provide users with anonymity, while solving many of the law enforcement problems that exist in a totally untraceable system. The ability to trace transactions in either direction can help law enforcement officials catch tax evaders and money launderers by revealing who has paid or who has been paid by the suspected criminal. Electronic blackmailers can be caught because the deposit numbers of the victim's ill-gotten coins could be decrypted, identifying the blackmailer when the money is deposited.

The ability to restore traceability does not solve one very important law enforcement problem, namely detecting forged coins. Backward tracing will help identify a forged coin if a particular payment or deposit (or depositor) is under suspicion. In that case, backward tracing will reveal the withdrawal number, allowing the originating bank to locate its withdrawal record and to verify the validity of the coin. If a forged coin makes its way into the system, however, it may not be detected until the bank whose money is being counterfeited realizes that the total value of its electronic cash deposits using a particular key exceeds the values of its withdrawals. The only way to determine which deposits are genuine and which are forged would require obtaining permission to decrypt the withdrawal numbers for

each deposit of electronic cash using the compromised key. This would violate the privacy that anonymous cash was designed to protect.

Unfortunately, the Stadler-Piveteau-Camenisch scheme is not efficient because it is based on the bulky cut-and-choose method. However, it may be possible to apply similar ideas to restore traceability in a more efficient electronic cash scheme.

CONCLUSION

This Essay has described several innovative payment schemes that provide user anonymity and payment untraceability. These electronic cash schemes have cryptographic mechanisms in place to address the problems of multiple spending and token forgery. Some serious concerns about the ability of an electronic cash system to recover from a security failure have been identified, however. Concerns about the impact of anonymity on money laundering and tax evasion also have been discussed.

Because it is simple to make an exact copy of an electronic coin, a secure electronic cash system must have a way to protect against multiple spending. If the system is implemented on-line, then multiple spending can be prevented by maintaining a database of spent coins and checking this list with each payment. If the system is implemented off-line, then there is no way to prevent multiple spending cryptographically, but it can be detected when the coins are deposited. Detection of multiple spending after the fact is useful only if the identity of the offender is revealed. Cryptographic solutions have been proposed that will reveal the identity of the multiple spender while preserving user anonymity.

Token forgery can be prevented in an electronic cash system as long as the cryptography is implemented soundly and securely, the secret keys used to sign coins are not compromised, and integrity is maintained on the public keys. If there is a security flaw or a key compromise, however, the anonymity of electronic cash will delay detection of the problem. Even after the existence of a compromise is detected, the Bank will not be able to distinguish its own valid coins from forged ones. Because there is no way to guarantee that the Bank's secret keys never will be compromised, it is important to limit the damage that a compromise could inflict. This could be accomplished by limiting the total value of coins issued with a particular key. Lowering these limits, however, also reduces the anonymity of the system as there is a smaller pool of coins associated with each key.

The untraceability property of electronic cash creates problems in detecting money laundering and tax evasion because there is no way to link the payer and payee. To counter this problem, it is possible to design a system that has an option to restore traceability using an escrow mechanism. If certain conditions are met (such as a court order), a deposit or withdrawal record can be turned over to a commonly trusted entity holding a key that can decrypt information connecting the deposit to a withdrawal or vice versa. This will identify the payer or payee in a particular transaction. It is not a solution to the token forgery problem, however, because there may be no way to know which deposits are suspect. In that case, identifying forged coins would require turning over all of the Bank's deposit records to the trusted entity to have the withdrawal numbers decrypted.

This Essay also has examined two optional features of off-line electronic cash: transferability and divisibility. Because the size of an electronic coin must grow with each transfer, the number of transfers allowed per coin must be limited. Also, allowing transfers magnifies the problems of detecting counterfeit coins, money laundering, and tax evasion. Coins can be made divisible without losing any security or anonymity features, but at the expense of additional memory requirements and transaction time.

In conclusion, the potential risks in electronic commerce are magnified when anonymity is present. Anonymity creates the potential for large sums of counterfeit money to go undetected by preventing identification of forged coins. Anonymity also provides an avenue for laundering money and evading taxes that is difficult to combat without resorting to escrow mechanisms. Anonymity can be provided at varying levels, but increasing the level of anonymity also increases the potential damages. It is necessary to weigh the need for anonymity with these concerns. It may well be concluded that these problems are best avoided by using a secure electronic payment system that provides privacy, but not anonymity.

EXHIBIT C

Constitution, NW., Washington, DC 20230 or via internet at *MClayton@doc.gov.*

Written comments and recommendations for the proposed information collection should be sent to David Rostker, OMB Desk Officer, Room 10202, New Executive Office Building, Washington, DC 20503 within 30 days of the publication of this notice in the **Federal Register**.

Dated: August 20, 2002.

Madeleine Clayton,

Departmental Paperwork Clearance Officer, Office of the Chief Information Officer

[FR Doc. 02–21602 Filed 8–23–02; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

Minority Business Development Agency

Online Performance Data Base

ACTION: Proposed collection; comment request.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites other Federal agencies and the general public to take this opportunity to comment on proposed or continuing information collections, as required by the Paperwork Reduction Act of 1995, Pub. L. 104–13 (44 U.S.C. 3506(c)(2)(A)).

DATES: Written comments must be submitted on or before October 25, 2002.

ADDRESSES: Direct all written comments to Madeleine Clayton, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6608, 14th and Constitution Avenue, NW., Washington, DC 20230 or via internet at *Mclayton@doc.gov.*

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection instrument and instructions should be directed to Juanita E. Berry, Department of Commerce, Minority Business Development Agency (MBDA), Room 5079, 14th and Constitution Avenue, NW., Washington, DC 20230, or call (202) 482–3262.

SUPPLEMENTARY INFORMATION:

I. Abstract

The Performance Database identifies minority business clients receiving Agency-sponsored business development services in the form of management and technical assistance, the kind of assistance each receives, and the impact of that assistance on the growth and profitability of the client firms. MBDA requires this information to monitor, evaluate, and plan Agency programs which effectively enhance the development of the minority business sector.

II. Method of Collection

Electronic transfer of performance data.

III. Data

OMB Number: 0640–0002.

Agency Form Number: N/A.

Type of Review: Extension of a currently approved collection.

Affected Public: State or local governments, individuals, and profit and non-profit institutions.

Estimated Number of Responses: 240 (approximately 50 respondents with numerous responses).

Estimated Time Per Response: 3–15 minutes per function, as needed (5 functions).

Estimated Total Annual Burden Hours: 4,818.

Estimated Total Annual Cost: $0 (software package is provided by MBDA).

IV. Request for Comments

Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and cost) of the proposed collection of information; (c) ways to enhance the quality, utility and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they will also become a matter of pubic record.

Dated: August 20, 2002.

Madeleine Clayton,

Departmental Paperwork Clearance Officer, Electronic Government Division, Office of the Chief Information Officer.

[FR Doc. 02–21601 Filed 8–23–02; 8:45 am]

BILLING CODE 3510–21–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 001214352–2097–02]

Announcing Approval of Federal Information Processing Standard (FIPS) 180–2, Secure Hash Standard; a Revision of FIPS 180–1

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice.

SUMMARY: The Secretary of Commerce has approved FIPS 180–2, Secure Hash Standard, and has determined that the standard is compulsory and binding on Federal agencies for the protection of sensitive, unclassified information.

FIPS 180–2, Secure Hash Standard, replaces FIPS 180–1, which was issued in 1992 and which specified an algorithm (SHA–1) for producing a 160-bit output called a message digest. The message digest is a condensed representation of electronic data and is used in cryptographic processes such as digital signatures and message authentication. FIPS 180–2 includes three additional algorithms, which produce 256-bit, 384-bit, and 512-bit message digests. These expanded capabilities are compatible with and support the strengthened security requirements of FIPS 197, Advanced Encryption Standard.

EFFECTIVE DATE: This standard is effective February 1, 2003.

Specifications: FIPS 180–2 is available on the NIST web page at: *http://csrc.nist.gov/encryption/tkhash.html.*

FOR FURTHER INFORMATION CONTACT: Ms. Elaine Barker, (301) 975–2911, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, Maryland 20899–8930. Email: *elaine.barker@nist.gov.*

SUPPLEMENTARY INFORMATION: A notice was published in the **Federal Register** (66 FR 29287) on May 30, 2001, announcing the proposed FIPS 180–2, Secure Hash Standard, for public review and comment. The **Federal Register** notice solicited comments from the public, academic and research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations. In addition to being published in the **Federal Register**, the notice was posted on the NIST web pages; information was provided about the submission of electronic comments. Comments and responses were received from three private sector organizations

or individuals, and from one federal government organization.

The comments raised technical issues related to the standard, asked for clarification of technical issues, and recommended editorial changes. None of the comments opposed the adoption of the revised Federal Information Processing Standard. All of the editorial and related comments were carefully reviewed, and changes were made to the standard where appropriate. NIST recommended that the Secretary approve FIPS 180–2. Following is an analysis of the comments received.

Comment: NIST should provide a security evaluation of the algorithms added to FIPS 180–2, and give the rationale for the various design choices. Such an analysis would increase confidence in the algorithms and facilitate external evaluation.

Response: The standard provides four secure hash algorithms, which differ in the number of bits of security provided for the data being processed. Secure hash algorithms are designed for use in conjunction with another algorithm, which may have requirements that the hash algorithm have a certain number of bits of security. For example, a digital signature algorithm that provides 128 bits of security may require that the secure hash algorithm also provide 128 bits of security.

NIST believes that these algorithms are secure because it is computationally infeasible to find a message that corresponds to a given message digest, or to find two different messages that produce the same message digest. It is highly probable that a change to a message will result in a different message digest.

FIPS 180–2 includes the technical specifications for the four algorithms that have been selected to provide 160, 256, 384 and 512 bits of security. NIST anticipates and invites external examination and scrutiny concerning the security of the algorithms.

Comment: NIST should include a note in the standard indicating whether SHA–256 could be truncated to 160 bits for use as an alternative to SHA–1 (also 160 bits).

Response: The use of hash functions will be addressed in application standards (*e.g.*, in the upcoming revision of Federal Information Processing Standard 186–2, the Digital Signature Standard).

Comment: NIST should mention in the standard that SHA–256 constants are easily extracted from the SHA–512 constants.

Response: NIST believes that the decisions concerning the use of constants and how to extract them should be made by those organizations that develop implementations of the standard.

Comment: One comment suggested that there may be weaknesses in the algorithms, and proposed a method to change the standard to address the perceived weaknesses.

Response: It would be more appropriate for the perceived weaknesses to be addressed in application standards such as the Federal Information Processing Standard for the Keyed-Hash Message Authentication Code (HMAC), which has been approved as FIPS 198, as opposed to addressing this in FIPS 180–2 itself. Furthermore, NIST expects to issue guidance on the implementation of secure hash functions.

Authority: Under section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, the Secretary of Commerce is authorized to approve standards and guidelines for the cost effective security and privacy of sensitive information processed by federal computer systems.

Executive Order 12866: This notice has been determined not to be significant for purposes of E.O. 12866.

Dated: August 19, 2002.

Karen Brown,

Deputy Director, NIST.

[FR Doc. 02–21599 Filed 8–23–02; 8:45 am]

BILLING CODE 3510–CN–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[Docket Number: 020729185–2185–01]

Announcement of Graduate Research Fellowships in the National Estuarine Research Reserve System for Fiscal Year 2003

AGENCY: Estuarine Reserves Division (ERD), Office of Ocean and Coastal Resource Management (OCRM), National Ocean Service (NOS), National Oceanic and Atmospheric Administration (NOAA), Department of Commerce (DOC).

ACTION: Notice.

SUMMARY: The Estuarine Reserves Division of OCRM is soliciting applications for graduate fellowship funding within the National Estuarine Research Reserve System. This notice sets forth funding priorities, selection criteria, and application procedures.

The National Estuarine Research Reserve System of NOAA announces the availability of graduate research fellowships. The Estuarine Reserves Division anticipates that 27 Graduate Research Fellowships will be competitively awarded to qualified graduate students whose research occurs within the boundaries of at least one reserve. Minority students are encouraged to apply. The amount of the fellowship is $17,500; at least 30% of total project cost match is required by the applicant. Applicants may apply for between one and three years of funding. Fellowships will start June 1, 2003. A later start date may be requested with justification and will be reviewed by ERD for approval.

DATES: Applications must be postmarked no later than November 1, 2002. Notification regarding the awarding of fellowships will be issued on or about March 1, 2003.

ADDRESSES: Erica Seiden, program coordinator, NOAA/Estuarine Reserves Division, 1305 East-West Highway, N/ORM5, SSMC4, 11616 Floor, Silver Spring, MD 20910, Attn: NERRS GRF. Phone: 301–713–3155 ext. 172 Fax: 301–713–4363, internet: *erica.seiden@noaa.gov.* Web page: *http://www.ocrm.nos.noaa.gov/nerr/fellow.html.* See Appendix I for National Estuarine Research Reserve addresses.

FOR FURTHER INFORMATION CONTACT: For further information on specific research opportunities at National Estuarine Research Reserves, contact the site staff listed in Appendix I or the program specialist listed in the Addresses section above. For application information, contact Erica Seiden of ERD (see contact information above).

SUPPLEMENTARY INFORMATION:

I. Authority and Background

Section 315 of the Coastal Zone Management Act of 1972, as amended (CZMA), 16 U.S.C. 1461, establishes the National Estuarine Research Reserve System (NERRS). 16 U.S.C. 1461 (e)(1)(B) authorizes the Secretary of Commerce to make grants to any coastal state or public or private person for purposes of supporting research and monitoring within a National Estuarine Research Reserve that are consistent with the research guidelines developed under subsection (c). This program is listed in the Catalog of Federal Domestic Assistance (CFDA) under ''Coastal Zone Management Estuarine Research Reserves,'' Number 11.420.

II. Information on the National Estuarine Research Reserve System

The National Estuarine Research Reserve System consists of estuarine areas of the United States and its territories which are designated and

EXHIBIT D

New Records in Collision Attacks on SHA-2

Yingxin Li[1], Fukang Liu[2], and Gaoli Wang[1](✉)

[1] Shanghai Key Laboratory of Trustworthy Computing, Software Engineering Institute, East China Normal University, Shanghai, China
liyx1140@163.com,glwang@sei.ecnu.edu.cn
[2] Tokyo Institute of Technology, Tokyo, Japan
liu.f.ad@m.titech.ac.jp

Abstract. The SHA-2 family including SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA512/256 is a U.S. federal standard published by NIST. Especially, there is no doubt that SHA-256 is one of the most important hash functions used in real-world applications. Due to its complex design compared with SHA-1, there is almost no progress in collision attacks on SHA-2 after ASIACRYPT 2015. In this work, we retake this challenge and aim to significantly improve collision attacks on the SHA-2 family. First, we observe from many existing attacks on SHA-2 that the current advanced tool to search for SHA-2 characteristics has reached the bottleneck. Specifically, longer differential characteristics could not be found, and this causes that the collision attack could not reach more steps. To address this issue, we adopt Liu et al.'s MILP-based method and implement it with SAT/SMT for SHA-2, where we also add more techniques to detect contradictions in SHA-2 characteristics. This answers an open problem left in Liu et al.'s paper to apply the technique to SHA-2. With this SAT/SMT-based tool, we search for SHA-2 characteristics by controlling its sparsity in a dedicated way. As a result, we successfully find the first practical semi-free-start (SFS) colliding message pair for 39-step SHA-256, improving the best 38-step SFS collision attack published at EUROCRYPT 2013. In addition, we also report the first practical free-start (FS) collision attack on 40-step SHA-224, while the previously best theoretic 40-step attack has time complexity 2^{110}. Moreover, for the first time, we can mount practical and theoretic collision attacks on 28-step and 31-step SHA-512, respectively, which improve the best collision attack only reaching 27 steps of SHA-512 at ASIACRYPT 2015. In a word, with new techniques to find SHA-2 characteristics, we have made some notable progress in the analysis of SHA-2 after the major achievements made at EUROCRYPT 2013 and ASIACRYPT 2015.

Keywords: practical collision attack · SHA-2 · SAT/SMT

1 Introduction

Before the devastating attacks in 2005 [37,38,39,40] on the MD-SHA hash family, there was a trend to design fast hash functions with a similar structure to MD4, including MD5, SHA-0, SHA-1, SHA-2, RIPEMD-128 and RIPEMD-160, just to

name a few. After 2005, we have witnessed efficient collision attacks on full MD4 [37], MD5 [39], SHA-0 [2,40], and SHA-1 [15,16,35,38] as well as the SFS collision attack on full RIPEMD-128 [14]. In spite of these successful attacks on the MD-SHA hash family, SHA-2 survived this game, mainly due to its more conservative and complex design. Since SHA-2 has been used worldwide, studying its collision and preimage resistances is always of practical interest, though it is also challenging.

Preimage attacks on SHA-2. In the past few years, there have been many results for the preimage attacks on SHA-256 and SHA-512. The first preimage attack on SHA-256 and SHA-512 [11] based on the meet-in-the-middle (MITM) technique reached 24 steps with a complexity of about 2^{240} and 2^{480}, respectively. These preimage attacks were significantly improved at ASIACRYPT 2009 [1], which were improved to 43-step SHA-256 and 46-step SHA-512, respectively. Then, at ASIACRYPT 2010, Guo et al. [9] presented advanced MITM preimage attacks on 42-step SHA-256 and SHA-512, respectively. At FSE 2012, the biclique technique was applied to find preimages of SHA-2 [12], where preimage attacks on 45-step SHA-256 and 50-step SHA-512 with time complexity of $2^{255.5}$ and $2^{511.5}$ were achieved, respectively. It should be noted that the authors in [12] also presented pseudo-preimage attacks on 52-step SHA-256 and 57-step SHA-512 with a complexity of 2^{255} and 2^{511}, respectively. However, all these preimage attacks are far from practical.

Distinguishing attacks on the compression function of SHA-2. Compared with preimage and collision attacks, distinguishing attacks are less meaningful for a hash function, though they can help better understand its security. At the rump session of EUROCRYPT 2008 [42], the non-randomness of 39-step SHA-256 was presented, and a practical example for 33 steps was given by Yu and Wang. In [10], free-start (FS) near-collisions for up to 31 steps of SHA-256 were presented. Then, Lamberger and Mendel gave a second-order differential attack on 46 steps of SHA-256 with a practical complexity in [13]. Later, this attack was extended to 47 steps of SHA-256 with a practical complexity at ASIACRYPT 2011 [3]. At INSCRYPT 2014 [41], Yu and Bai further utilized the attack strategy in [3] to mount a practical distinguishing attack on 48 steps of SHA-512.

Collision attacks on SHA-2. The first practical collision attack on SHA-256 [29] was presented at FSE 2006, only reaching 18 steps. At FSE 2008, Nikolic and Biryukov [32] improved this practical attack to 21 steps, and they also gave a SFS collision attack on 23 steps of SHA-256. This attack was later further extended to 24 steps of SHA-256 and SHA-512 in [10,33]. Then, at ASIACRYPT 2011, the first major improvement was achieved, where the advanced guess-and-determine (GnD) technique to search for SHA-2 characteristics was invented [25], and the SFS collision for 32-step SHA-256 and the collision for 27-step SHA-256 were presented, respectively. After this work at ASIACRYPT 2011, this advanced automatic tool has been gradually improved in 3 papers published at EUROCRYPT 2013 [27], FSE 2014 [8] and ASIACRYPT 2015 [6]. In addition, much

more complex message differences are used to mount (FS/SFS) collision attacks on SHA-2 in these 3 papers. A summary of these collision attacks is shown in Table 1.

Automatic tools to search for SHA-2 characteristics. Although major achievements have been made in collision attacks on SHA-2 in [6,8,25,27], the corresponding advanced automatic tool to find SHA-2 characteristics is not open-source. Due to the complex design of SHA-2, this significantly increased the difficulty to follow these works without this tool, let alone to improve this tool. Although Stevens open sourced his dedicated tools [34,35,36] to find MD5 and SHA-1 characteristics, they could not be applied to SHA-2 as SHA-2 is too complex, and contradictions easily occur in its differential characteristics [25]. Recently, to make finding collision-generating signed differential characteristics easier, Liu et al. invented a novel MILP-based method [23] and it works quite well for RIPEMD-160. As can be observed in [23], two main techniques are how to describe signed difference transitions through each component of the step function and how to automatically detect contradictions in an efficient way. At the end of [23], the authors left an interesting problem whether it is possible to apply this technique to SHA-2 because it is required for the model to detect more contradictions in SHA-2 characteristics.

Our contributions. We briefly summarize our contributions as follows:

1. We demonstrate for the first time that the technique developed in [23] can be applied to SHA-2, and this obviously gives a positive answer to the question left in [23]. Specifically, we develop a SAT/SMT-based tool to efficiently search for valid SHA-2 differential characteristics based on the technique to search for signed differential characteristics in [23] and the technique to automatically verify the correctness of a differential characteristic in [20].
2. We shed new insight into the (free-start/semi-free-start) collision attacks on SHA-2. For the first time, we are able to propose:
   - the first practical SFS colliding message pair for 39-step SHA-256, breaking the record of 38 steps kept by Mendel et al. at EUROCRYPT 2013 [27] after 10 years;
   - the first practical free-start colliding message pair for 40-step SHA-224, improving the previously best theoretic 40-step attack with time complexity 2^{110} published at FSE 2012 [17];
   - the first practical colliding message pair for 28-step SHA-512, updating the previously best record given at ASIACRYPT 2015 [6] by 1 step.
   - the first collision attack on 31-step SHA-512 with time complexity $2^{115.6}$, improving the previously best one published at ASIACRYPT 2015 [6] by 4 steps.

In addition to these notable progress, we also improved the best collision attack on 31-step SHA-256 published at EUROCRYPT 2013 [27], reducing the time complexity from $2^{65.5}$ to $2^{49.8}$. Our results are summarized in Table 1. Especially, we note that there is gap between the previous (SFS) collision attacks

on SHA-256 and SHA-512. Specially, due to the similarity between SHA-256 and SHA-512, a (SFS) collision attack on r steps of SHA-256 should have been applicable to r steps of SHA-512, and vice versa. However, this is not the case in previous attacks, as shown in Table 1. We believe this is caused by the infeasibility to find the corresponding valid SHA-2 characteristics with the current GnD technique. Based on our new technique, we have made the (SFS) collision attacks on SHA-256 and SHA-512 reach the same number of steps.

Moreover, based on our results for SHA-2, it indicates that the SAT/SMT-based method performs much better than the dedicated but non-open-source ones developed in [6,8,25,27]. This also contradicts the claims made in [8] that the performance of SAT-based method for SHA-2 is bad. Note that our SAT/SMT-based method is completely different from the one used in [8], which simply uses a model to describe two parallel instances of the value transitions as in [31].

Table 1. Summary of collision attacks on SHA-2, where FS collision* denotes the free-start collision without considering padding, and SFS collision denotes the semi-free-start collision.

State size	Hash size	Attack type	Steps	Time	Memory	References	Year
256	All	collision	28	*practical*	\	[27]	2013
			31	$2^{65.5}$	2^{34}	[27]	2013
			31	$2^{49.8}$	2^{48}	**Sect. 4.2**	**2023**
		SFS collision	38	*practical*	\	[27]	2013
			39	***practical***	\	**Sect. 4.1**	**2023**
	256	FS collision	52	$2^{127.5}$	\	[17]	2012
	224	FS collision*	39	*practical*	\	[6]	2015
		FS collision	40	2^{110}	\	[17]	2012
		FS collision*	**40**	***practical***	\	**Sect. 4.5**	**2023**
512	All	collision	27	*practical*	\	[6]	2015
			28	***practical***	\	**Sect. 4.4**	**2023**
			31	$2^{115.6}$	$2^{77.3}$	**Sect. 4.3**	**2023**
		SFS collision	38	*practical*	\	[8]	2014
			39	*practical*	\	[6]	2015
	384	FS collision	40	2^{183}	\	[17]	2012
		FS collision*	41	*practical*	\	[6]	2015
	256	FS collision*	43	*practical*	\	[6]	2015
	224	FS collision*	44	*practical*	\	[6]	2015

The source code to search for the differential characteristics and verify the (SFS/FS) collisions for SHA-256 and SHA-512 is available at https://github.com/Peace9911/sha_2_attack.git

Outline. This paper is organized as follows. The notations and some preliminary works of this paper are introduced in Section 2. A high-level overview of how to implement the MILP-based method with an SAT/SMT-based method and how to overcome more contradictions in the differential characteristics of SHA-2 in is given Section 3. Then, we show how to find the differential characteristics to mount the (SFS/FS) collisions for SHA-2 in Section 4. Finally, we conclude this paper in Section 5.

2 Preliminaries

2.1 Notations

For a better understanding of this paper, we introduce the following notations.

1. $\boxplus$ and $\boxminus$ represent modulo addition and modulo subtraction on 32/64 bits, respectively.
2. $\gg$, $\ggg$, $\oplus$, $\neg$, $\vee$ and $\wedge$ represent *shift right*, *rotate right*, *exclusive or*, *not*, *or*, and *and*, respectively.
3. $x[i]$ denotes the i-th bit of x and $x[0]$ is the least significant bit.
4. δx denotes the modular difference, i.e., $\delta x = x' \boxminus x$.
5. Δx denotes the signed difference between x' and x. We use the same notation as in [21,23], i.e.,

$$\Delta x[i] = \begin{cases} \mathtt{n} & (x[i] = 0, x'[i] = 1) \\ \mathtt{u} & (x[i] = 1, x'[i] = 0) \\ \mathtt{=} & (x[i] = x'[i]) \\ \mathtt{0} & (x[i] = x'[i] = 0) \\ \mathtt{1} & (x[i] = x'[i] = 1) \end{cases} \tag{1}$$

6. $M = (m_0, m_1, \ldots, m_{15})$ and $M' = (m'_0, m'_1, \ldots, m'_{15})$ represent two message blocks.

Definition 1. *[23] The signed difference Δx is said to be an expansion of the modular difference δx only when Δx corresponds to the modular difference δx.*

Definition 2. *[23] The hamming weight of the signed difference Δx is denoted by $\mathbf{H}(\Delta x)$ and $\mathbf{H}(\Delta x)$ is the number of indices i such that $\Delta x[i] \in \{n, u\}$.*

For example, let

$$\Delta x_0 = [\texttt{==== nu== ==== ==== ==== ==== ==== ====}],$$
$$\Delta x_1 = [\texttt{==== =n== ==== ==== ==== ==== ==== ====}].$$

Then, both Δx_0 and Δx_1 are the expansions of $\delta x = 2^{26}$. Moreover, we have $\mathbf{H}(\Delta x_0) = 2$ and $\mathbf{H}(\Delta x_1) = 1$. As each signed difference corresponds to a unique modular difference, for convenience, when computing $\delta x \boxplus \delta y$ for a given $(\Delta x, \Delta y)$, we also simply denote $\delta x \boxplus \delta y$ by $\Delta x \boxplus \Delta y$. For the above example, we have $\Delta x_0 \boxplus \Delta x_1 = 2^{27}$.

2.2 Description of SHA-2

The SHA-2 family is a series of hash functions standardized by NIST as part of the Secure Hash Standard (SHS) [7]. This family mainly consists of two versions, namely SHA-256 and SHA-512. Furthermore, NIST defines a general truncation procedure for SHA-256 and SHA-512, which includes SHA-224, SHA-512/224, SHA-512/256 and SHA-384. SHA-2 adopts the well-known Merkle-Damgård construction [5,30], and its compression functions employ the Davies-Meyer construction. As the two main versions of SHA-2, SHA-256 and SHA-512 have 32-bit and 64-bit state words, respectively. SHA-256 and SHA-512 utilize 512-bit message words and 1024-bit message words as input, with their chaining variables and final outputs being 256 bits and 512 bits, respectively.

The compression functions of SHA-256 and SHA-512 are computed through iterative updates to internal states. The number of steps, which is denoted by r, is 64 for SHA-256 and 80 for SHA-512. In the following, we provide a brief overview of their compression functions. They consist of two main parts: the message expansion and the state update transformation. A complete description of SHA-2 is given in [7].

Message Expansion. The 512-bit message block for SHA-256 and the 1024-bit message block for SHA-512 are divided into 16 message words of sizes 32 bits and 64 bits, respectively, which are denoted by $(m_1, \ldots, m_{15})$. Then, the 16 message words are expanded to r expanded message words W_i, i.e., $W_0, W_1, \ldots, W_{r-1}$:

$$W_i = \begin{cases} m_i & 0 \le i \le 15, \\ \sigma_1(W_{i-2}) \boxplus W_{i-7} \boxplus \sigma_0(W_{i-15}) \boxplus W_{i-16} & 16 \le i \le r-1. \end{cases}$$

The functions $\sigma_0(x)$ and $\sigma_1(x)$ in SHA-256 are given by

$$\sigma_0(x) = (x \ggg 7) \oplus (x \ggg 18) \oplus (x \gg 3),$$
$$\sigma_1(x) = (x \ggg 17) \oplus (x \ggg 19) \oplus (x \gg 10).$$

The functions $\sigma_0(x)$ and $\sigma_1(x)$ in SHA-512 are given by

$$\sigma_0(x) = (x \ggg 1) \oplus (x \ggg 8) \oplus (x \gg 7),$$
$$\sigma_1(x) = (x \ggg 19) \oplus (x \ggg 61) \oplus (x \gg 6).$$

State update transformation. We utilize the alternate description for the state update of SHA-256 and SHA-512, as illustrated in Figure 1.

The state update transformation starts from a 256-bit (resp. 512-bit) chaining value $iv = (A_{-1}, \ldots, A_{-4}, E_{-1}, \ldots, E_{-4})$ for SHA-256 (resp. SHA-512), and updates it by applying the step function r times. In each step $i = 0, \ldots, r-1$, one expanded message word W_i is used to compute the two state words E_i and A_i as follows, where K_i is a predefined constant and can be referred to [7].

$$E_i = A_{i-4} \boxplus E_{i-4} \boxplus \Sigma_1(E_{i-1}) \boxplus \mathrm{IF}(E_{i-1}, E_{i-2}, E_{i-3}) \boxplus K_i \boxplus W_i,$$
$$A_i = E_i \boxminus A_{i-4} \boxplus \Sigma_0(A_{i-1}) \boxplus \mathrm{MAJ}(A_{i-1}, A_{i-2}, A_{i-3}).$$

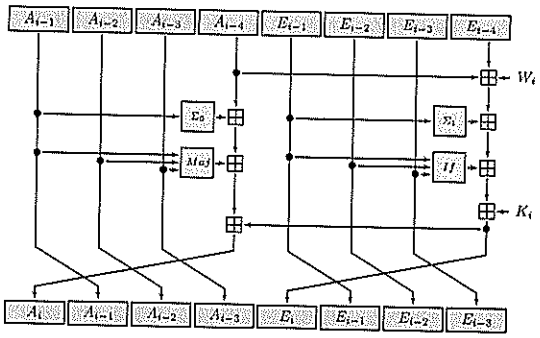


Fig. 1. The state update transformation of SHA-2.

Both SHA-256 and SHA-512 utilize the same Boolean functions IF and MAJ, as defined below:

$$\mathrm{IF}(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus z,$$
$$\mathrm{MAJ}(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z).$$

However, the linear functions Σ_0 and Σ_1 are different for SHA-256 and SHA-512. For SHA-256, they are defined below:

$$\Sigma_0(x) = (x \ggg 2) \oplus (x \ggg 13) \oplus (x \ggg 22),$$
$$\Sigma_1(x) = (x \ggg 6) \oplus (x \ggg 11) \oplus (x \ggg 25).$$

For SHA-512, they are defined below:

$$\Sigma_0(x) = (x \ggg 28) \oplus (x \ggg 34) \oplus (x \ggg 39),$$
$$\Sigma_1(x) = (x \ggg 14) \oplus (x \ggg 18) \oplus (x \ggg 41).$$

After the last step of the state update transformation, the previous chaining value is added to the output of the state update. The result of this feed-forward sum is the chaining value h:

$$h = (A_{63} \boxplus A_{-1}, \ldots, A_{60} \boxplus A_{-4}, E_{63} \boxplus E_{-1}, \ldots, E_{60} \boxplus E_{-4}).$$

On finding (FS/SFS) collisions. Denote the compression function of SHA-2 by $h_i = H(h_{i-1}, M_i)$. To find a collision with j message blocks, we need to find $(M_1, \ldots, M_j)$ and $(M'_1, \ldots, M'_j) \neq (M_1, \ldots, M_j)$ such that $h_j = h'_j$ where $h'_i = H(h'_{i-1}, M'_i)$ and $h_0 = h'_0$ is a *predefined constant*. In most cases, only $M_j \neq M'_j$ is required and we have $M_k = M'_k$ for $1 \leq k < j$. To find SFS collisions, we need to find $H(h, M) = H(h, M')$ where $M \neq M'$ and h can be an *arbitrary value*. To find FS collisions, we need to find $H(h, M) = H(h', M')$ where $M \neq M'$ and (h, h') can be *arbitrary values*.

2.3 Previous Methods to Search for Differential Characteristics

Almost all effective collision attacks on the MD-SHA hash family rely on Wang et al.'s techniques [37,38,39]. One of the most important steps is to find a collision-generating differential characteristic. For this purpose, there are three methods in the literature, as summarized below.

- **Hand-crafted method:** This remarkable work was first done by Wang et al. in their ground-breaking works on MD4 [37], MD5 [39], SHA-0 [40], and SHA-1 [38]. However, for complex designs like SHA-256 and RIPEMD-160, finding such differential characteristics for a large number of steps by hand is almost impossible, or at least considerably time-consuming.
- **Ad-hoc heuristic search tools:** De Cannière and Rechberger developed the first heuristic search tool for this problem based on the guess-and-determine (GnD) technique, and successfully applied it to SHA-1 [4]. Subsequently, this heuristic search tool were further developed and it has been applied to many hash functions like RIPEMD-128, RIPEMD-160, SHA-256, and SHA-512 [6,8,14,18,19,22,24,25,26,27,28]. However, the implementation of this GnD-based tool is not open-source. Although Stevens made his tools for MD5 and SHA-1 [34,35,36] open-source, it requires a significant amount of work to tweak them for SHA-2 because contradictions much more easily occur in the differential characteristics of SHA-2, and no existing tools for SHA-2 are based on this method.
- **Off-the-shelf solvers:** The method was first explored in [31] with SAT solvers after Wang et al.'s attacks and it was later also applied to SHA-1 in [35]. The main idea is to construct a model to describe two parallel instances of the value transitions. A new MILP-based method proposed by Liu et al. [23] is to model the pure signed difference transitions through each component of the round function, aided with some contradiction-detecting techniques. Especially, this technique [23] works quite well for RIPEMD-160.

3 SAT/SMT-based Tools for the MD-SHA Hash Family

The first SAT-based method to find collision-generating differential characteristics was proposed in 2006 [31], but the model is to simply describe two parallel instances of the value transitions. To efficiently capture the information of the signed difference propagation, the MILP-based method was proposed in [23]. Although the authors of [23] only target RIPEMD-160, since the MD-SHA hash functions share similar structures, the authors also mention that there are indeed much more applications beyond RIPEMD-160. Especially, whether it is applicable to SHA-2 is left as an interesting problem.

We answer this question in this paper. First, we show how to implement the MILP-based method [23] with an SAT/SMT-based method, and how to detect more contradictions in SHA-2 characteristics. Then, we demonstrate how to utilize our tools to find suitable differential characteristics to significantly improve the (SFS) collision attacks on SHA-2.

For the MILP-based method in [23], the constraints are already in Conjunctive Normal Form (CNF) due to the usage of the software Friday, which can output the minimized CNF for a given truth table with the Quine-McCluskey (QM) algorithm. However, they choose to further convert CNF into linear inequalities in order to use the solver Gurobi [23]. In this sense, we can not claim any novelty for how to re-implement the propagation of signed difference transitions with SAT/SMT. To make this paper self-contained, we briefly describe the idea to model the signed difference propagation with SAT/SMT. Note that when applying it to searching for valid SHA-2 characteristics, nontrivial additional techniques are required, as can be seen later in our detailed description of the search strategy.

For the MD-SHA hash family, it can be observed that in their round functions, there are three basic operations:

- modular addition;
- logic shift;
- Boolean functions.

Hence, we only describe how to describe the signed difference transitions through the modular addition and Boolean functions. For the logic shift, it does affect the model for RIPEMD-160 as shown in [23]. However, in the case of SHA-2, there is no such problem and it only affects the order of the variables. Hence, we simply omit it in this section.

Since we will target both SHA-256 and SHA-512, and their state sizes are 32 and 64 bits, respectively, to make the description of the model general, we treat the state size as n bits, i.e., the modular addition is within modulo 2^n.

3.1 SAT/SMT Models for the Signed Difference Transitions

Similar to [23], we use 2 binary variables (v, d) to describe the signed difference. Specifically, $(0,0)$, $(0,1)$ and $(1,1)$ correspond to `[=]`, `[n]` and `[u]`, respectively, while we always exclude $(1,0)$ as it carries the same information as $(0,0)$. For the n-bit signed difference Δx, throughout this paper, the signed difference at the i-th $(0 \leq i \leq n-1)$ bit is always represented by $(x_v[i], x_d[i])$. For example, if $n = 5$ and $\Delta x =$ `[=u==n]`, we have

$$(x_v[0], x_d[0]) = (0,0), (x_v[1], x_d[1]) = (1,1), (x_v[2], x_d[2]) = (0,0),$$
$$(x_v[3], x_d[3]) = (0,0), (x_v[4], x_d[4]) = (0,1).$$

Modelling the modular addition. As explained in [23], given the signed difference Δx and Δy, it is sufficient to pick only 1 signed difference Δz to describe the modular difference $\delta z = \delta x \boxplus \delta y$.

To achieved this, the intermediate variable Δc with $\Delta c[0] =$ `[=]` is introduced and the propagation rules for

$$(\Delta x[i], \Delta y[i], \Delta c[i]) \xrightarrow{Add} (\Delta z[i], \Delta c[i+1])$$

Table 2. The propagation rules for $(\Delta x[i], \Delta y[i], \Delta c[i]) \xrightarrow{Add} (\Delta z[i], \Delta c[i+1])$ in [23]

[=== → ==],	[==n → n=],	[==u → u=],	[=n= → n=],				
[=u= → u=],	[=nn → =n],	[=un → ==],	[=nu → ==],				
[=uu → =u],	[n== → n=],	[u== → u=],	[n=n → =n],				
[u=n → ==],	[n=u → ==],	[u=u → =u],	[nn= → =n],				
[nun → n=],	[unn → n=],	[nnu → n=],	[uun → u=],				
[unu → u=],	[nuu → u=],	[uuu → uu].					

are shown in Table 2, where $0 \leq i \leq n-1$.

With the above method to describe the signed difference, there are 27 possible values for

$$(x_v[i], x_d[i], y_v[i], y_d[i], c_v[i], c_d[i], z_v[i], z_d[i], c_v[i+1], c_d[i+1])$$

based on Table 2. With the software LogicFriday, we can obtain the corresponding CNF to describe that this tuple can only take these 27 possible values. For convenience, we denote the CNF by $\mathcal{C}_{\texttt{Add}}(i)$. In this way, the complete model for the modular addition can be described with $\mathcal{C}_{Add}(i)$ for $0 \leq i \leq n-1$ and $(c_v[0], c_d[0]) = (0, 0)$.

For convenience, we denote the model for the modular addition $\delta z = \delta x \boxplus \delta y$ by $\mathcal{C}_{Add}(\Delta x, \Delta y, \Delta z, \Delta c)$.

Modelling the expansions of the modular difference [23]. In the above model, the signed difference transition through the modular addition is deterministic. To obtain all possible signed differences corresponding to the same modular difference, the authors of [23] introduce a model to describe the expansions of the modular difference. Given one Δz, the aim is to find all possible $\Delta\xi$ such that $\delta\xi = \delta z$, i.e., $\Delta\xi$ and Δz correspond to the same modular difference. To achieve this, as in [23], an intermediate variable Δc is introduced and there are two methods to model it, as shown in Table 3.

Table 3. Two methods to describe the propagation rules for the expansion of modular difference [23]

Method 1 $(\Delta z[i], \Delta c[i]) \xrightarrow{Exp} (\Delta\xi[i], \Delta c[i+1])$	[nn → =n], [uu → =u], [nu → ==], [un → ==], [n= → n=], [n= → un], [u= → u=], [u= → nu], [=n → n=], [=n → un], [=u → u=], [=u → nu], [== → ==].
Method 2 $(\Delta\xi[i], \Delta z[i], \Delta c[i]) \xrightarrow{Exp} (\Delta c[i+1])$	[=un → n], [=nn → =], [=uu → =], [=nu → u], [u=n → =], [n=n → n], [u=u → u], [n=u → =], [nu= → n], [nn= → =], [uu= → =], [un= → u], [=== → =].

Similarly, based on the above way to describe the signed difference and using the software LogicFriday, the corresponding CNF to describe the constraints on

$$(z_v[i], z_d[i], c_v[i], c_d[i], \xi_v[i], \xi_d[i], c_v[i+1], c_d[i+1])$$

for Method 1 can be obtained, which is denoted by $\mathcal{C}_{Exp}(i)$. The complete model for the expansion of the modular difference is thus $\mathcal{C}_{Exp}(i)$ for $0 \leq i \leq n-1$ and $(c_v[0], c_d[0]) = (0, 0)$ for Method 1.

In the same way, we can also obtain the corresponding CNF denoted by $\mathcal{C}'_{Exp}(i)$ to describe the constraints on

$$(\xi_v[i], \xi_d[i], z_v[i], z_d[i], c_v[i], c_d[i], c_v[i+1], c_d[i+1])$$

for Method 2. The complete model for the expansion of the modular difference is thus $\mathcal{C}'_{Exp}(i)$ for $0 \leq i \leq n-1$ and $(c_v[0], c_d[0]) = (0, 0)$ for Method 2.

For convenience, we denote the model for the expansions of the modular addition in Method 1 and Method 2 by $\mathcal{C}_{Exp}(\Delta z, \Delta\xi, \Delta c)$ and $\mathcal{C}'_{Exp}(\Delta z, \Delta\xi, \Delta c)$.

Modelling the vectorial Boolean functions $w = f(x, y, z)$ [23]. In SHA-2, there are some vectorial Boolean functions, i.e., f can be XOR, IF or MAJ where $XOR(x, y, z) = x \oplus y \oplus z$. Note that σ_0, σ_1, Σ_0 and Σ_1 in SHA-2 are basically the same as XOR. Generally speaking, we can have

$$w[i] = f_i(x[i], y[i], z[i])$$

where f_i is a Boolean function $\mathbb{F}_2^3 \mapsto \mathbb{F}_2$ and $0 \leq i \leq n-1$. As described in [23], there are two models for $(f_i)_{0 \leq i \leq n-1}$: (i) the fast filtering model; (ii) the full model.

For the fast filtering model, we first need to build a table to include all valid propagation rules for $(\Delta x[i], \Delta y[i], \Delta z[i], \Delta w[i])$ and then obtain the corresponding valid values for

$$(x_v[i], x_d[i], y_v[i], y_d[i], z_v[i], z_d[i], w_v[i], w_d[i]).$$

Finally, LogicFriday is used to obtain the corresponding CNF for the constraints on this tuple.

For the full model, we need to involve both the signed difference and bit values. Specifically, the first step is to list all possible propagation rules for

$$(\Delta x[i], \Delta y[i], \Delta z[i], \Delta w[i], x[i], y[i], z[i]),$$

where $(x[i], y[i], z[i])$ can make the signed difference transition

$$(\Delta x[i], \Delta y[i], \Delta z[i]) \xrightarrow{f_i} \Delta w[i]$$

hold with probability 1. Then, we can obtain all the possible valid values for

$$(x_v[i], x_d[i], y_v[i], y_d[i], z_v[i], z_d[i], w_v[i], w_d[i], x[i], y[i], z[i]).$$

Finally, with LogicFriday, we obtain the corresponding CNF to describe the constraints on this tuple.

For convenience, we denote the fast filtering model and full model for $w = f(x, y, z)$ by $\mathcal{C}^f_{fast}(\Delta x, \Delta y, \Delta z, \Delta w)$ and $\mathcal{C}^f_{full}(\Delta x, \Delta y, \Delta z, \Delta w, x, y, z)$, respectively.

3.2 SAT/SMT Models for the Value Transitions

In SHA-2, contradictions easily occur in the collision-generating differential characteristics. To avoid this, we use the technique proposed by Liu et al. at CRYPTO 2020 [20]: using one model for the differential characteristic and another model for the value transitions. In the above model for the differential characteristic, we have included the relations between the value and the differential characteristic if using the full model for the Boolean functions. Specially, if the full model is applied to step i, the conditions on the internal states at step $i-1$, $i-2$ and $i-3$ to ensure the difference transitions have been added. Then, we can further build a model to optionally describe how to compute the internal state $i-1$ or $i-2$ or $i-3$ in order to test whether these conditions can hold, which is the model for the value transitions. It is easy to build the model for the value transitions as we only need to model the modular addition and Boolean functions.

To compute $z = x \boxplus y$, we can simply introduce a variable c with $c[0] = 0$ to denote the carry. Then, we list all possible values for the tuple $(x[i], y[i], c[i], z[i])$ and get the corresponding CNF for the model addition. For convenience, we denote the model for the modular addition of the value by $\mathcal{C}^{Add}_{Val}(x, y, z, c)$.

To compute $w = f(x, y, z)$, we can simply list all possible valid values for the tuple $(x[i], y[i], z[i], w[i])$ and get the corresponding CNF. For convenience, the model for the vectorial Boolean function f is denoted by $\mathcal{C}^f_{Val}(x, y, z, c)$.

With the two basic models $\mathcal{C}^{Add}_{Val}$ and $\mathcal{C}^f_{val}$, we can simply build the model for the value transitions through the step function of SHA-2 by decomposing the step function with intermediate variables. For convenience, the models to compute E_i, A_i and W_i are denoted by $\mathcal{C}^E_{Val}(i)$, $\mathcal{C}^A_{Val}(i)$ and $\mathcal{C}^W_{Val}(i)$, respectively.

Remark 1. With the model for value transitions, we can also use it to search for conforming input pairs for some dense parts of the differential characteristic. Specially, after a differential characteristic is obtained, we first derive all the differential conditions. Then, to find the conforming input pairs for the dense part of the characteristic, we simply use the value transitions for this part and add the corresponding differential conditions on the internal states to the model. This will be frequently used in our attacks in order to search for conforming message pairs automatically. Indeed, it is not surprising that this method has been used in [20,31].

3.3 Models for SHA-2

we can give a high-level description of the model for the step function of SHA-2, as shown in Algorithm 1. In this algorithm, we implicitly introduce many intermediate variables $(\Delta B_{i,j}, \Delta C_{i,j})$, where $\Delta B_{i,j}$ is used to decompose the step

function and $\Delta C_{i,j}$ is used to denote the carry. Their concrete meanings should be clear from the context. In addition, we also provide several optional parameters (OP1,OP2,OP3,OP4,OP5,OP6,OP7,OP8) to control the search strategy to increase the flexibility of the model.

4 New (SFS/FS) Collision Attacks on SHA-2

In the (FS/SFS) collision attacks on SHA-2 [6,8,25,27] with the GnD tools, a crucial step is to first search for a relatively complex local collision in the message expansion, where nonzero message differences exist in the middle steps, and the differences will be cancelled in as many consecutive steps as possible in the forward and backward directions.

Basically, after determining the local collision in the message expansion, the number of attacked steps is also known. However, finding a valid attack further requires attackers to finish the following two tasks:

Task 1: searching for a corresponding differential characteristic in (A_i, E_i);
Task 2: finding the conforming message pair to ensure the validity of the differential characteristic since contradictions easily occur.

In some cases, even though we know there may exist a good local collision in the message expansion, it may be still infeasible to find a valid attack due to the difficulty of Task 1 or Task 2. For example, the SFS collision attack can reach 39 steps of SHA-512, but could not reach 39 steps of SHA-256. Moreover, the best collision attack on SHA-256 could reach 31 steps, while it is only 27 steps for SHA-512.

4.1 The First Practical SFS Collision for 39-Step SHA-256

We note that there is a practical SFS collision attack on 39-step SHA-512 published at ASIACRYPT 2015 [6]. However, the authors did not report any attacks on 39-step SHA-256, even though SHA-256 and SHA-512 share almost the same message expansion and state update function, i.e., only with different state sizes and different rotation numbers in Σ and σ. Specifically, the strategy to construct the local collision for 39-step SHA-512 should have been applicable to 39-step SHA-256, and this cannot be the bottleneck. We thus believe that the difficulty exists in either Task 1 or Task 2.

Hence, we aim to retake this challenge with the new SAT/SMT-based technique. First, we observe that in the differential characteristic for 39-step SHA-512 in [6], the local collision spans over 19 steps (steps 8–26), and the nonzero message differences exist in 9 words $(W_8, \ldots, W_{12}, W_{16}, W_{17}, W_{24}, W_{26})$. In addition, in (W_{26}, W_{17}, A_{18}), there is only a one-bit difference, respectively.

In our new attack on 39-step SHA-256, we use the same strategy to construct the local collision, as shown in Figure 2(a). Different from the ad-hoc GnD techniques [6,8,27], it is efficient to use our SAT/SMT-based technique to find a sparse differential characteristic by minimizing the Hamming weight of the signed

Algorithm 1 High-level description of the model for the step function of SHA-2

procedure SHA2(i,OP1,OP2,OP3,OP4,OP5,OP6,OP7,OP8)
  SHA2-E(i,OP1,OP2,OP3)
  SHA2-A(i,OP4,OP5,OP6)
  if $i \geq 16$ **then**
    SHA2-W(i,OP7)
  if OP8==1 **then**
    $\mathcal{C}^{E}_{Val}(i)$, $\mathcal{C}^{A}_{Val}(i)$, $\mathcal{C}^{W}_{Val}(i)$
procedure SHA2-E(i,OP1,OP2,OP3)
  $\mathcal{C}_{Add}(\Delta A_{i-4}, \Delta W_i, \Delta B_{i,0}, \Delta C_{i,0})$
  $\mathcal{C}_{Add}(\Delta E_{i-4}, \Delta B_{i,0}, \Delta B_{i,1}, \Delta C_{i,1})$
  $E^{s}_{i-1} = E_{i-1} \ggg s$,
  if OP1==1 **then** $\mathcal{C}^{XOR}_{fast}(\Delta E^{2}_{i-1}, \Delta E^{13}_{i-1}, \Delta E^{22}_{i-1}, \Delta B_{i,2})$
  else
    $\mathcal{C}^{XOR}_{full}(\Delta E^{2}_{i-1}, \Delta E^{13}_{i-1}, \Delta E^{22}_{i-1}, \Delta B_{i,2}, E^{2}_{i-1}, E^{13}_{i-1}, E^{22}_{i-1})$
  $\mathcal{C}_{Add}(\Delta B_{i,1}, \Delta B_{i,2}, \Delta B_{i,3}, \Delta C_{i,2})$
  if OP2==1 **then** $\mathcal{C}^{IF}_{fast}(\Delta E_{i-1}, \Delta E_{i-2}, \Delta E_{i-3}, \Delta B_{i,4})$
  else
    $\mathcal{C}^{IF}_{full}(\Delta E_{i-1}, \Delta E_{i-2}, \Delta E_{i-3}, \Delta B_{i,4}, E_{i-1}, E_{i-2}, E_{i-3})$
  $\mathcal{C}_{Add}(\Delta B_{i,3}, \Delta B_{i,4}, \Delta B_{i,5}, \Delta C_{i,3})$
  if OP3==1 **then** $\mathcal{C}_{Exp}(\Delta B_{i,5}, \Delta E_i, \Delta C_{i,4})$
  else
    $\mathcal{C}'_{Exp}(\Delta B_{i,5}, \Delta E_i, \Delta C_{i,4})$
procedure SHA2-A(i,OP4,OP5,OP6)
  $A^{s}_{i-1} = A_{i-1} \ggg s$,
  if OP4==1 **then** $\mathcal{C}^{XOR}_{fast}(\Delta A^{6}_{i-1}, \Delta A^{11}_{i-1}, \Delta A^{25}_{i-1}, \Delta B_{i,6})$
  else
    $\mathcal{C}^{XOR}_{full}(\Delta A^{6}_{i-1}, \Delta A^{11}_{i-1}, \Delta A^{25}_{i-1}, \Delta B_{i,6}, A^{6}_{i-1}, A^{11}_{i-1}, A^{25}_{i-1})$
  if OP5==1 **then** $\mathcal{C}^{MAJ}_{fast}(\Delta A_{i-1}, \Delta A_{i-2}, \Delta A_{i-3}, \Delta B_{i,7})$
  else
    $\mathcal{C}^{MAJ}_{full}(\Delta A_{i-1}, \Delta A_{i-2}, \Delta A_{i-3}, \Delta B_{i,7}, A_{i-1}, A_{i-2}, A_{i-3})$
  $\mathcal{C}_{Add}(\Delta B_{i,6}, \Delta B_{i,7}, \Delta B_{i,8}, \Delta C_{i,5})$
  $\mathcal{C}_{Add}(\Delta A_{i-4}, \Delta B_{i,8}, \Delta B_{i,9}, \Delta C_{i,6})$
  $\mathcal{C}_{Add}(\Delta A_{i,9}, \Delta B_{i,10}, \Delta E_i, \Delta C_{i,7})$
  if OP6==1 **then** $\mathcal{C}_{Exp}(\Delta B_{i,10}, \Delta A_i, \Delta C_{i,8})$
  else
    $\mathcal{C}'_{Exp}(\Delta B_{i,10}, \Delta A_i, \Delta C_{i,8})$
procedure SHA2-W(i,OP7)
  $W^{s}_{i-2} = W_{i-2} \ggg s, {W^{s}_{i-2}}' = W_{i-2} \gg s$,
  $\mathcal{C}^{XOR}_{full}(\Delta W^{17}_{i-2}, \Delta W^{19}_{i-2}, \Delta {W^{10}_{i-2}}', \Delta B_{i,10}, W^{17}_{i-2}, W^{19}_{i-2}, {W^{10}_{i-2}}')$
  $W^{s}_{i-15} = W_{i-15} \ggg s, {W^{s}_{i-15}}' = W_{i-15} \gg s$,
  $\mathcal{C}^{XOR}_{full}(\Delta W^{7}_{i-15}, \Delta W^{18}_{i-15}, \Delta {W^{3}_{i-15}}', \Delta B_{i,11}, W^{7}_{i-15}, W^{18}_{i-15}, {W^{3}_{i-15}}')$
  $\mathcal{C}_{Add}(\Delta B_{i,10}, \Delta W_{i-7}, \Delta B_{i,12}, \Delta C_{i,9})$
  $\mathcal{C}_{Add}(\Delta B_{i,11}, \Delta B_{i,12}, \Delta B_{i,13}, \Delta C_{i,10})$
  $\mathcal{C}_{Add}(\Delta B_{i,13}, \Delta W_{i-16}, \Delta B_{i,14}, \Delta C_{i,11})$
  if OP7==1 **then** $\mathcal{C}_{Exp}(\Delta B_{i,14}, \Delta W_i, \Delta C_{i,12})$
  else
    $\mathcal{C}'_{Exp}(\Delta B_{i,14}, \Delta W_i, \Delta C_{i,12})$

differences. This is crucial to improve the uncontrolled differential probability and to make the message modification more practical. Our general procedure to search for the differential characteristic for 39-step SHA-256 is summarized below:

Step 1: **Minimize the Hamming weight of ΔW_i.** Specifically, find the minimal value of $t_w = \sum_{i=0}^{38} \mathbf{H}(\Delta W_i)$ such that the nonzero differences only exist in the 9 expanded message words $(W_8, \ldots, W_{12}, W_{16}, W_{17}, W_{24}, W_{26})$. Note that the concrete message differences are not specified at this step and the only goal is to find the minimal value t_w.

Step 2: **Minimize the Hamming weight of ΔA_i.** Specifically, under the conditions

$$\begin{aligned} \forall i \in [19, 38]: \ \delta A_i = 0, \\ \forall i \in [23, 38]: \ \delta E_i = 0, \\ \forall i \in [0, 38] \text{ and } i \notin \{8, \ldots, 12, 16, 17, 24, 26\}: \delta W_i = 0, \\ \sum_{i=0}^{38} \mathbf{H}(\Delta W_i) = t_w, \end{aligned}$$

find the minimal value of $t_A = \sum_{i=0}^{38} \mathbf{H}(\Delta A_i)$ such that there exists a solution of a 39-step collision-generating differential characteristic, i.e., there is a solution to $(\Delta W_i, \Delta A_i, \Delta E_i)$ for $0 \le i \le 38$ to allow a 39-step attack. Still, we only aim at the minimal value t_A, and do not fix $(\Delta W_i, \Delta A_i, \Delta E_i)$ according to the solution at this step.

Step 3: **Minimize the Hamming weight of ΔE_i.** In addition to the conditions at Step 2, we further add the condition

$$\sum_{i=0}^{38} \mathbf{H}(\Delta A_i) = t_A.$$

Under these conditions, find and output the solution of $(\Delta W_i, \Delta A_i, \Delta E_i)$ for $0 \le i \le 38$ that minimizes $\sum_{i=0}^{38} \mathbf{H}(\Delta E_i)$.

Following the above procedure, we successfully found a corresponding 39-step differential characteristic, as shown in Table 4. By our procedure, this differential characteristic can be kept as sparse as possible and hence it is expected to be valid.

Remark 2. Our strategy to search for a concrete 39-step differential characteristic is different from the GnD technique in [6] because we first minimize the Hamming weight of $(\Delta W_i, \Delta A_i)$ and then search the solution under such constraints. However, there is no such a minimization procedure when searching for the differential characteristic in 39-step SHA-512 in [6]. Without this strategy, the differential characteristic may be dense and there is a high chance that it is invalid, which may somehow explain why the technique in [6] failed for 39-step SHA-256.

Message modification. As the differential characteristic is still relatively dense, we could not ensure that there must exist a conforming message pair. To verify this, we first extract all the constraints on $(A_i, E_i)_{-4 \le i \le 22}$ and $(W_i)_{0 \le i \le 38}$ for this differential characteristic. Then add these constraints to the SAT/SMT model for the value transitions of SHA-256, and solve the model to find a solution of these variables. We succeed in finding a practical SFS colliding message pair for 39-step SHA-256 in 120 seconds with 26 threads, as shown in Table 5.

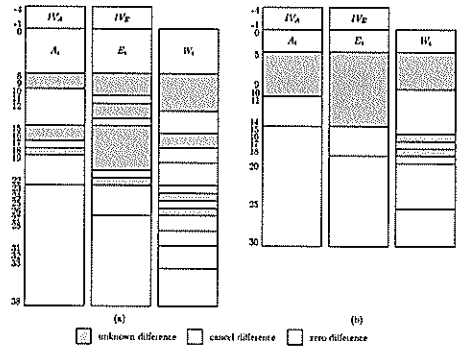


Fig. 2. (a) represent the shape of the 39-step differential SHA-256 and (b) represent the shape of the differential characteristic for 31-step SHA-256

4.2 Improved Collision Attacks on 31-Step SHA-256

The best existing collision attack on SHA-256 reaches 31 steps, which was published at EUROCRYPT 2013 [27]. The main idea is to use a two-block method to convert a SFS collision into a collision by utilizing the available degrees of freedom in the first few message words. To achieve this purpose, the first step is to find a suitable differential characteristic for 31-step SHA-256. In [27], this 31-step differential characteristic relies on a properly constructed local collision in the message expansion, which spans over 14 steps (steps 5−18). Specifically, the nonzero message differences only exist in 7 expanded message words

$$(W_5, W_6, W_7, W_8, W_9, W_{16}, W_{18}).$$

Moreover, there are no conditions on the first 5 expanded message words $(W_i)_{0 \le i \le 4}$ and hence they can be freely chosen to efficiently convert a SFS collision into a collision. The shape of the 31-step differential characteristic is shown in Figure 2(b).

The method in [27] to convert SFS collisions into collisions is described below:

Step 1: Find 2^ℓ solutions of $(A_i)_{-3 \le i \le 12}$, $(E_i)_{1 \le i \le 12}$ and $(W_i)_{5 \le i \le 12}$ that satisfy the differential conditions on steps 5−12. Store them in a table denoted by $\mathtt{TAB}_1$.

Table 4. The differential characteristic for 39 steps of SHA-256

i	ΔA_i	ΔE_i	ΔW_i
-4	================================	================================	
-3	================================	================================	
-2	================================	================================	
-1	================================	================================	
0	================================	================================	================================
1	================================	================================	================================
2	================================	================================	================================
3	================================	================================	================================
4	================================	================================	================================
5	================================	================================	================================
6	================================	===0============================	================================
7	================================	===1==========11====11======0===	================================
8	===u============================	unnn1=1110=0=0101==00011==11110=	===u============================
9	================n=u====u======n===	010n0n0111010nu0100iun011ni0n=10	======n===u==========u==========
10	================================	0101iuin=1n0n010=u0=11nuu=1u00=n1	===n============================
11	================================	=100010000=0101=0===0010=10=1=0=	======nn==========n===n==nn=uu=n
12	================================	=unn010000=1000011=00011==0=101=	============u======nn==========
13	================================	10110nuuuuuuuuu0u101un000010n111	================================
14	================================	=111=0000000000=0=1=001111111=1=	================================
15	============================n===	1100110110100000000inuuuuuuuu001	================================
16	=======u=u=======u==============	0101000unu000001001u1000110unn=n1	======n===u==========u==========
17	================================	1100111u00nn=100110=u1u00unn000n	===n============================
18	===n============================	uuu1uuuuu01000=110n000111101=0101	================================
19	================================	000u0n1000101=0un01=1100=u11n000	================================
20	================================	011100un0u001unnnn11000000001111	================================
21	================================	=110=111=0==000=1=======1==1===	================================
22	================================	=nuu==0110==00101=0110=====110=	================================
23	================================	=000===========================	================================
24	================================	=111============================	=======n=n=======n==============
25	================================	================================	================================
26	================================	================================	===u============================
27	================================	================================	================================
28	================================	================================	================================
29	================================	================================	================================
30	================================	================================	================================
31	================================	================================	================================
32	================================	================================	================================
33	================================	================================	================================
34	================================	================================	================================
35	================================	================================	================================
36	================================	================================	================================
37	================================	================================	================================
38	================================	================================	================================

Table 5. The SFS colliding message pair for 39 steps of SHA-256

cv	02b19d5a 88e1df04 5ea3c7b7 f2f7d1a4 86cb1b1f c8ee51a5 1b4d0541 651b92e7
M	c61d6de7 755336e8 5e61d618 18036de6 a79f2f1d f2b44c7b 4c0ef36b a85d45cf f72b8c2f 0def947c a0eab159 8021370c 4b0d8011 7aad07f6 33cd6902 3bad5d64
M'	c61d6de7 755336e8 5e61d618 18036de6 a79f2f1d f2b44c7b 4c0ef36b a85d45cf e72b8c2f 0fcf907c b0eab159 81a1bfc1 4b098611 7aad07f6 33cd6902 3bad5d64
hash	431cadcd ce6893bb d6c9689a 334854e8 3baae1ab 038a195a ccf54a19 1c40606d

Step 2: Compute $2^{96-\ell}$ arbitrary first message blocks and get $2^{96-\ell}$ chaining inputs $(A_{-4},\ldots,A_{-1})$ and $(E_{-4},\ldots,E_{-1})$. Check $\mathtt{TAB}_1$ and find a match in (A_{-3},A_{-2},A_{-1}). Then, $(W_i)_{0\le i\le 4}$ and E_0 are all determined for this match.

Step 3: At this step, $(W_i)_{0\le i\le 12}$ have been fixed. Use the degrees of freedom in (W_{13},W_{14},W_{15}) to fulfill the remaining uncontrolled conditions on $(E_{13},E_{14},E_{15},W_{16},W_{18})$. If it fails, go to Step 2.

Supposing Step 3 succeeds with probability $2^{-\gamma}$, the time complexity for this two-block method to find a collision is $2^{96-\ell+\gamma}+2^{\ell}\cdot T_{\mathtt{tool}}$, where $T_{\mathtt{tool}}$ denotes the time to find a solution of $(A_i)_{-3\le i\le 12}$, $(E_i)_{1\le i\le 12}$ and $(W_i)_{5\le i\le 12}$ at Step 1. The memory complexity is 2^{ℓ}. In [27], $\ell\approx 34$, $\gamma\approx 3.5$ and $T_{\mathtt{tool}}$ is negligible. Hence the time complexity is estimated as $2^{65.5}$ and the memory complexity is 2^{34}.

According to the above analysis, it is clear that ℓ and γ should be improved to get better attacks. Moreover, the best time-memory trade-off cannot be achieved with their 31-step differential characteristic [27]. Note that the maximal value of ℓ is dominated by the number of differential conditions on steps 5−12 and hence we can expect a relatively larger ℓ with a sparser differential characteristic. Therefore, we are interested whether it is possible to find a new sparser differential characteristic with our tool that can help achieve the optimal time-memory trade-off, i.e., with time and memory complexity close to $2^{96/2}=2^{48}$. The overall searching procedure is stated as follows:

1. **Minimize the Hamming weight of ΔW_i.** Specifically, find the minimal value of $t_w=\sum_{i=0}^{30}\mathbf{H}(\Delta W_i)$ while keeping the minimal $\mathbf{H}(\Delta W_{16})$ and the minimal $\mathbf{H}(\Delta W_{18})$ such that the nonzero differences only exist in the 7 expanded message words $(W_5,W_6,W_7,W_8,W_9,W_{16},W_{18})$. Note that the concrete message differences are not specified at this step.
2. **Minimize the Hamming weight of ΔA_i.** Specifically, under the conditions
$$\begin{aligned}\forall i\in[11,30]:\ \delta A_i=0,\\ \forall i\in[15,30]:\ \delta E_i=0,\\ \forall i\in[0,30]\ \text{and}\ i\notin\{5,\ldots,9,16,18\}:\delta W_i=0,\\ \sum_{i=0}^{30}\mathbf{H}(\Delta W_i)=t_w,\end{aligned}$$
find the minimal value of $t_A=\sum_{i=0}^{30}\mathbf{H}(\Delta A_i)$ such that there is a solution to $(\Delta W_i,\Delta A_i,\Delta E_i)$ for $0\le i\le 30$ to allow a 31-step attack. Still, we only aim at the minimal value t_A, and do not fix $(\Delta W_i,\Delta A_i,\Delta E_i)$ according to the solution at this step.
3. **Minimize the Hamming weight of ΔE_i.** In addition to the conditions at Step 2, we further add the condition
$$\sum_{i=0}^{30}\mathbf{H}(\Delta A_i)=t_A.$$

Under these conditions, find and output the solution minimizing $\sum_{i=0}^{30} \mathbf{H}(\Delta E_i)$ to allow a 31-step attack.

As already mentioned in our SAT/SMT models, to further detect the contradictions caused by the complex relationship between (A_i, E_i, W_i), we sometimes add the value transitions at certain steps to ensure its validity. In our model for the 31-step differential characteristic, this strategy is applied to $(A_i, E_i, W_i)_{7\le i\le 10}$. Without this strategy, we found that the obtained differential characteristic was indeed invalid[3]. Our new 31-step differential characteristic is shown in Table 6.

Estimating ℓ and γ. We use a dedicated method to find valid solutions of $(A_i)_{-3\le i\le 12}$, $(E_i)_{1\le i\le 12}$ and $(W_i)_{5\le i\le 12}$ such that ℓ can be better estimated. First, use the model for the value transitions to find a solution of $(A_i)_{1\le i\le 12}$, $(E_i)_{5\le i\le 12}$ and $(W_i)_{9\le i\le 12}$ that satisfy the differential conditions on steps 5−12. For simplicity, this solution is called a starting point for 31-step SHA-256. Due to

$$A_i = E_i \boxminus A_{i-4} \boxplus \Sigma_0(A_{i-1}) \boxplus \mathrm{MAJ}(A_{i-1}, A_{i-2}, A_{i-3}), \tag{2}$$

$(A_{-3},\ A_{-2},\ A_{-1},\ A_0)$ will then depend on $(E_1,\ E_2,\ E_3,\ E_4)$ for this starting point. Moreover, according to

$$E_i = A_{i-4} \boxplus E_{i-4} \boxplus \Sigma_1(E_{i-1}) \boxplus \mathrm{IF}(E_{i-1}, E_{i-2}, E_{i-3}) \boxplus K_i \boxplus W_i, \tag{3}$$

$(E_1,\ E_2,\ E_3,\ E_4)$ will depend on $(W_5,\ W_6,\ W_7,\ W_8)$ for this starting point. By analyzing the conditions on $(W_5,\ W_6,\ W_7,\ W_8)$ to ensure the local collision in the message expansion, we find that there are in total 2^{14}, 2^{23}, 2^{27} and 2^{25} possible values of W_5, W_6, W_7 and W_8, respectively. Since there are no conditions on (E_1, E_2) or $(A_{-3},\ A_{-2},\ A_{-1},\ A_0)$ for this differential characteristic to hold, we only need to check how many (W_7, W_8) are left to ensure the conditions on (E_3, E_4) for this starting point. Experiments suggest that there are 2^{11} valid (W_7, W_8) left. Hence, based on this starting point, we can expect to generate $2^{14+23+11} = 2^{48}$ valid solutions of $(A_i)_{-3\le i\le 12}$, $(E_i)_{1\le i\le 12}$ and $(W_i)_{5\le i\le 12}$. For γ, since we do not have enough degrees of freedom in (W_{13}, W_{14}, W_{15}), we found that $\gamma \approx 1.3$ by 100 tests. If we can generate 2^{ℓ_1} starting points, then we have $2^{\ell} = 2^{\ell_1+48}$. Hence, the time complexity of the new collision attack on 31-step SHA-256 is estimated as

$$2^{96-48-\ell_1+1.3} + 2^{48+\ell_1} + 2^{\ell_1} \cdot T_{\mathtt{model}},$$

where $T_{\mathtt{model}} \approx 2^{31.7}$ denotes the time to generate a starting point and is always negligible. With $\ell_1 = 0$, i.e., only using one starting point, the time complexity is about $2^{49.8}$ and the memory complexity is 2^{48}. With this improved attack, we are much closer to a practical collision attack on 31-step SHA-256 and the bottleneck is the memory consumption. A possible practical implementation is to use less memory at the cost of increased time complexity.

[3] When searching for the differential characteristic for 39-step SHA-256, this strategy was not applied because we found that the obtained differential characteristic was valid.

Table 6. The differential characteristic for 31 steps of SHA-256

i	ΔA_i	ΔE_i	ΔW_i
-4	================================	================================	
-3	================================	================================	
-2	================================	================================	
-1	================================	================================	
0	================================	================================	================================
1	================================	================================	================================
2	================================	================================	================================
3	================================	==========================10====	================================
4	================================	==========0===0=========01==0	================================
5	==========n=unnnnnnn=n=	0001110100011111110nu=11111unnnu1	================nuuu=======0=uu=
6	========n=========u	101011=11=-0n0=-u11110==1110011n	==========u=====u==u=======n===u
7	===u===n=n=========n=========n=u	un0ui100n=01u11111001u1=n110u10n	=u=u=======n=====n=nu=n=====nun=
8	========================n==	1u01un0u0=1=1=11n=0=u0=001001u0=	=u=nn==========u==u===u==1======
9	==========================	01100001110=0=010===00=11101u0=1	================u==========1=u==
10	==================u==========	=1n1uuuuu0100=1un0=10unnnnnnn010	================================
11	================================	=01ui010uu1==11100===1000001n=0=	================================
12	================================	==110001=11===1n===0011110n=0=	================================
13	================================	===0====01======1================	================================
14	========================u=======	==========u==========0u==	================================
15	================================	================0==========1==	================================
16	================================	================1==========1==	==========unnnunnnnnnnnnnn==
17	================================	================================	================================
18	================================	================================	==============1=n=0==========n==
19	================================	================================	================================
20	================================	================================	================================
21	================================	================================	================================
22	================================	================================	================================
23	================================	================================	================================
24	================================	================================	================================
25	================================	================================	================================
26	================================	================================	================================
27	================================	================================	================================
28	================================	================================	================================
29	================================	================================	================================
30	================================	================================	================================

4.3 The First Collision Attack on 31-Step SHA-512

While the best existing collision attack on SHA-256 reaches 31 steps, the best collision attack on SHA-512 could only reach up to 27 steps, which was reported at ASIACRYPT 2015 [6]. The authors also stated in [6] that they could not find better collision attacks on SHA-512 because they could not find a suitable differential characteristic with their tools. In this part, we show how to overcome this obstacle.

Our practical SFS collision attack on 39-step SHA-256 benefits much from the practical SFS collision attack on 39-step SHA-512 due to their similarity. Hence, we feel interested to know whether it is possible to find a suitable differential characteristic for 31-step SHA-512 based on the collision attack on 31-step SHA-256 [27] with our new tool.

Specifically, similar to the 31-step attack on SHA-256, the nonzero message differences are injected in

$$(W_5, W_6, W_7, W_8, W_9, W_{16}, W_{18}),$$

and the local collision in the message expansion spans over 14 steps (steps 5−28), as shown in Figure 2(b). Similar to the collision attack on 31-step SHA-256, we first find SFS collisions and then convert them into collisions with the two-block method. The general procedure to convert SFS collisions into collisions is essentially the same and we refer the readers to the above improved attack on 31-step SHA-256.

The most challenging step to achieve the collision attack on 31-step SHA-512 is how to find a valid differential characteristic. In what follows, we describe how to use our tool to solve this problem.

Step 1: Find a solution of $(\Delta W_i)_{0\le i\le 30}$ with the minimal $\sum_{i=0}^{30}\mathbf{H}(\Delta W_i)$, while keeping the minimal $\mathbf{H}(\Delta W_{16})$ and the minimal $\mathbf{H}(\Delta W_{18})$, which allows a local collision in the message expansion.

Step 2: With the fixed solution of $(\Delta W_i)_{0\le i\le 30}$ obtained at Step 1, find a valid solution of $(\Delta A_i, \Delta E_i)_{0\le i\le 30}$, which follows the shape of the 31-step differential characteristic shown in Figure 2(b). Here, set a threshold to $\sum_{i=0}^{30}\mathbf{H}(\Delta A_i)$. Specifically, choose an integer tr and add the constraint

$$\sum_{i=0}^{30}\mathbf{H}(\Delta A_i) \le tr$$

to the model. If the solver cannot output a solution in a reasonable time, e.g., 72 hours, increase tr until a valid solution of $(\Delta A_i, \Delta E_i)_{0\le i\le 30}$ is found. Keep the solution of $(\Delta A_i)_{0\le i\le 30}$.

Step 3: With the fixed solution of $(\Delta A_i, \Delta W_i)_{0\le i\le 30}$, find a valid solution of $(\Delta E_i)_{0\le i\le 30}$ with the minimal $\sum_{i=0}^{30}\mathbf{H}(\Delta E_i)$, which allows a 31-step collision attack.

It is found that the obtained 31-step differential characteristic is invalid. Therefore, we propose to use the following method to correct this obtained solution.

Step 1: Set $(\Delta E_i)_{5\le i\le 7}$ as unknown variables. For the remaining $(\Delta E_i)_{0\le i\le 30}$ where $i \notin \{5,6,7\}$, keep them the same as those in the obtained solution. For $(\Delta A_i)_{0\le i\le 30}$ and $(\Delta W_i)_{0\le i\le 30}$, they are also kept the same as those in the obtained solution.

Step 2: Add the constraints describing the value transitions for $(A_i, E_i, W_i)_{7\le i\le 12}$ to the model.

In summary, we utilize the degrees of freedom in $(\Delta A_i, \Delta E_i)_{5\le i\le 7}$ and the model for value transitions to correct an invalid 31-step differential characteristic. In our search, the corresponding 31-step differential characteristic is shown in Table 7.

Complexity evaluation. As already mentioned, the only challenge to achieve the collision attack on 31-step SHA-512 is to find a suitable differential characteristic. Once it is found, the two-block method for 31-step SHA-256 can be directly applied. For consistency, we use the same notation, i.e., use (ℓ, γ, ℓ_1) to describe the time complexity and memory complexity as in the above collision attack on 31-step SHA-256. For our 31-step differential characteristic, there are in total 2^{36}, 2^{26}, 2^{25} and 2^{43} possible values for W_5, W_6, W_7 and W_8, respectively. For each starting point, i.e., the solution of $(A_i)_{1\le i\le 12}$, $(E_i)_{5\le i\le 12}$ and $(W_i)_{9\le i\le 12}$, we have experimentally found that there are on average $2^{15.3}$ possible (W_7, W_8) that can make the conditions on (E_3, E_4) hold. Therefore, for each starting point, we can generate $2^{36+26+15.3} = 2^{77.3}$ candidate solutions of $(A_i)_{-3\le i\le 12}$, $(E_i)_{1\le i\le 12}$ and $(W_i)_{5\le i\le 12}$. For 2^{ℓ_1} starting points, we thus can expect to generate $2^{\ell} = 2^{\ell_1+77.3}$ such many solutions. For γ, similarly, we found $\gamma \approx 0.9$ according to 100 experiments. Since the time complexity to generate a starting point is negligible, the whole time complexity is estimated as

$$2^{64\times 3-(\ell_1+77.3)+0.9} + 2^{\ell_1+77.3}$$

and the memory complexity is $2^{\ell_1+77.3}$. With $\ell_1 = 0$, i.e., only one starting point, the time and memory complexity are $2^{115.6}$ and $2^{77.3}$, respectively.

4.4 The Practical Collision Attack on 28-Step SHA-512

Similar to the 28-step attack on SHA-256 [27], the nonzero message differences are injected in

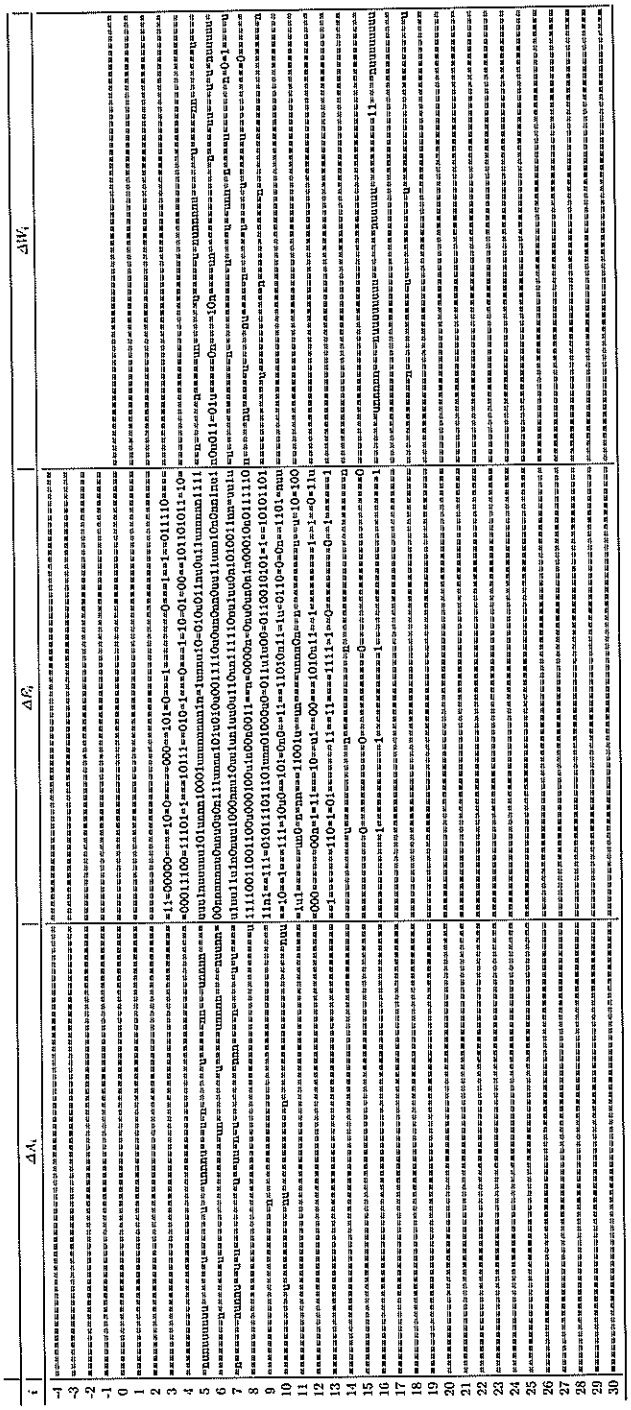
$$(W_8, W_9, W_{13}, W_{16}, W_{18}),$$

and the local collision in the message expansion spans over 11 steps (steps 8−18), resulting in a collision on 28-step SHA-512.

The most challenging step to achieve the collision attack on 28-step SHA-512 is how to find a valid differential characteristic. In what follows, we describe how to use our tool to solve this problem.

Step 1: Find a solution of $(\Delta W_i)_{0\le i\le 27}$ with the minimal $\sum_{i=0}^{27} \mathbf{H}(\Delta W_i)$ while keeping the minimal $\mathbf{H}(\Delta W_{16})$ and the minimal $\mathbf{H}(\Delta W_{18})$, which allows a local collision in the message expansion.

Table 7. The differential characteristic for 31-step SHA-512



Step 2: **Find the suitable ΔE_i.** With the fixed solution of $(\Delta W_i)_{0\leq i\leq 27}$ obtained at Step 1, find a valid solution of $(\Delta A_i, \Delta E_i)_{0\leq i\leq 27}$.

To improve the efficiency of the message modification, we have tried three strategies for Step 2, as detailed below:

Strategy 1: First, with the fixed solution of $(\Delta W_i)_{0\leq i\leq 27}$, find a valid solution of $(\Delta A_i, \Delta E_i)_{0\leq i\leq 27}$, and we minimize $\sum_{i=0}^{27} \mathbf{H}(\Delta A_i)$.
Then, with the fixed solution of $(\Delta W_i, \Delta A_i)_{0\leq i\leq 27}$, find a valid solution of $(\Delta E_i)_{0\leq i\leq 27}$ with the minimal $\sum_{i=0}^{27} \mathbf{H}(\Delta E_i)$.
Strategy 2: With the fixed solution of $(\Delta W_i)_{0\leq i\leq 27}$, find a valid solution of $(\Delta A_i, \Delta E_i)_{0\leq i\leq 27}$, and we minimize $\sum_{i=0}^{27} \mathbf{H}(\Delta E_i)$.
Strategy 3: With the fixed solution of $(\Delta W_i)_{0\leq i\leq 27}$, find a valid solution of $(\Delta A_i, \Delta E_i)_{0\leq i\leq 27}$, and we minimize $\sum_{i=11}^{27} \mathbf{H}(\Delta E_i)$.

After testing, it is found that Strategy 3 is more suitable for message modifications. However, such a 28-step differential characteristic is invalid. Similar to the method to correct the SHA-512 31-step differential characteristic, we also use the same technique to correct this invalid 28-step differential characteristic.

Step 1: Set $(\Delta E_i)_{8\leq i\leq 10}$ as unknown variables. For the remaining $(\Delta E_i)_{0\leq i\leq 27}$ where $i \notin \{8, 9, 10\}$, keep them the same as those in the obtained solution. For $(\Delta A_i)_{0\leq i\leq 27}$ and $(\Delta W_i)_{0\leq i\leq 27}$, they are also kept the same as those in the obtained solution.
Step 2: Add the constraints describing the value transitions for $(A_i, E_i, W_i)_{10\leq i\leq 12}$ to the model.

With this method, we eventually found a valid 28-step differential characteristic, as shown in Table 8.

Message modification. We use a different message modification technique than in [27]. In our message modification technique, we first determine all expanded message words and state variables in steps 8−12. Since the first 8 message words can be (almost) freely chosen, it is easy to connect the $(A_i, E_i)_{-4\leq i\leq -1}$ and $(A_i, E_i)_{8\leq i\leq 12}$ by using $(W_i)_{0\leq i\leq 7}$. Currently, $(A_i, E_i)_{-4\leq i\leq 12}$ and $(W_i)_{0\leq i\leq 12}$ has been determined. Then, the degree of freedom in message words $W_{13} - W_{15}$ can be used to fulfill the conditions on $E_{13} - E_{15}$ and (W_{16}, W_{18}). With this method, the cost to find the colliding message pair is almost negligible. The colliding message pair is shown in Table 9.

4.5 The First Practical FS Collision for 40-step SHA-224

In SHA-224, the last one output word $(E_{60} + E_{-4})$ was truncated. Therefore, similar to [6], we inject differences in E_{-4} to mount a FS collision attack. The best practical FS collision attack on SHA-224 was presented in [6] and it reaches

Table 8. The differential characteristic for 28-step SHA-512

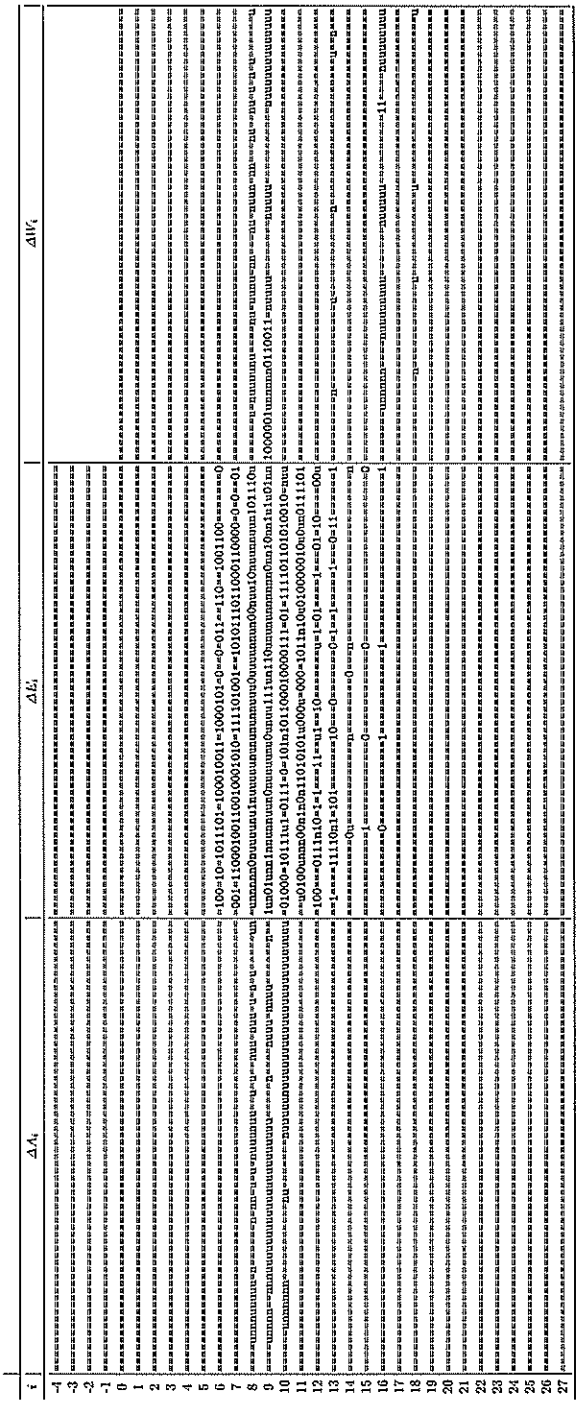


Table 9. The colliding message pair for 28 steps of SHA-512

M	1f736d69a0368ef6 7277e5081ad1c198 e953a3cdc4cbe577 bd05f6a203b2f75f
	dd18b3e39f563fca cad0a5bb69049fcd 4d0dd2a06e2efdc0 86db19c26fc2e1cf
	0184949e92cdd314 82fb3c1420112000 e4930d9b8295ab26 5500d3a2f30a3402
	26f0aa8790cb1813 a9c09c5c5015bc0d 53892c5a64e94edb 8e60d500013a1932
M'	1f736d69a0368ef6 7277e5081ad1c198 e953a3cdc4cbe577 bd05f6a203b2f75f
	dd18b3e39f563fca cad0a5bb69049fcd 4d0dd2a06e2efdc0 86db19c26fc2e1cf
	037a8f464c0bb995 83033bd41e111fff e4930d9b8295ab26 5500d3a2f30a3402
	26f0aa8790cb1813 a9809e5c4015bc45 53892c5a64e94edb 8e60d500013a1932
hash	dceb3d88adf54bd2 966c4cb1ab0cf400 01e701fdf10ab603 796d6e5028a5e89a
	f29a7517b216c09f 46dbae73b1db8cce 8ea44d45041010ea 26a7a6b902f2632f

39 steps. With our tool, we could find a practical FS collision for 40-step SHA-224 for the first time. Specifically, we inject message differences at 10 expanded words

$$(W_0, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{17}, W_{18}, W_{25}, W_{27}),$$

and then search for the corresponding 40-step differential characteristic. The searching strategy is almost the same as in our attack on 39-step SHA-256.

The 40-step differential characteristic and the conforming message pair are shown in Table 10 and Table 11, respectively.

5 Summary and Future Work

Although there was major progress on collision attacks on SHA-2 between 2011 and 2015, which essentially benefited from the development of the GnD technique to search for SHA-2 characteristics, no other progress has been made for nearly 8 years. One reason we believe is that the GnD technique has reached the bottleneck. In addition, the code for this GnD technique is not open source, which may further increase the difficulty to follow these works. Given the importance of SHA-2, there is no doubt that advancing the understanding of its collision resistance is always of practical interest.

By this work, we report for the first time that it is possible to overcome the obstacle to find SHA-2 characteristics with a SAT/SMT-based method, which is supported by several new improved attacks on the SHA-2 family. As can be observed, these new attacks highly depend on our SAT/SMT-based tool and how to use it in a dedicated way. Especially, we could find useful SHA-2 characteristics that could not be found with the GnD technique.

Through this work, we also expect that there could be more efforts to further improve this SAT/SMT-based method in the future, and that more and more researchers can easily perform analysis of SHA-2 with our tool.

Acknowledgement. We would like to thank the anonymous reviewers for their insightful comments. Yingxin Li and Gaoli Wang are supported by the National

Table 10. The differential characteristic for 40 steps of SHA-224

i	ΔA_i	ΔE_i	ΔW_i
-4	==========	==u==========	
-3	==========	==========	
-2	==========	==========	
-1	==========	==========	
0	==========	==========	==n==========
1	==========	==========	==========
2	==========	==========	==========
3	==========	==========	==========
4	==========	==========	==========
5	==========	==========	==========
6	==========	==========	==========
7	==========	0111======	==========
8	==========	1000=======10=====1==1==1===	==========
9	==u==========	unnn1=0=00=0=00=01=1=100=0110=1=	===u==========
10	==========n=u===u=====n===	100n0n110111=nu0001iun10in11n=00	=====n=u=========u==========
11	==========	0101u0n=1n0n010=u0=10nun=1u01=n1	===n==========
12	==========	=1000100001000l=0==0110=10=1=0=	======nn======n==n=u==nn=u=u=u
13	==========	=unn00000001100011=00011==0=101=	==========u=======nn==========
14	==========	11100nuuuuuuuuu1u=01un000001n001	==========
15	==========	=111=0000000000=0=1=001111111=1=	==========
16	==========n===	1100110110100000010inuuuuuuuu001	==========
17	=======u=u=======u==========	010100unu000001001ui000110unn=n1	======n===u==========u==========
18	==========	1100111u00nn=100110=uiu00unn000n	===n==========
19	===n==========	uuu1uuuu01000=110n000111101=0101	==========
20	==========	000u0n1000101=0un01=1100=u1in000	==========
21	==========	011100un1u001unnnn1100000001011l	==========
22	==========	=110=111=0==i1101=======1==1===	==========
23	==========	=nuu==0110===00101=0110=====110=	==========
24	==========	=000==========	==========
25	==========	=111==========	========n=n=======n==========
26	==========	==========	==========
27	==========	==========	===u==========
28	==========	==========	==========
29	==========	==========	==========
30	==========	==========	==========
31	==========	==========	==========
32	==========	==========	==========
33	==========	==========	==========
34	==========	==========	==========
35	==========	==========	==========
36	==========	==========	==========
37	==========	==========	==========
38	==========	==========	==========
39	==========	==========	==========

Table 11. The FS colliding message pair for 40 steps of SHA-224

CV	791c9c6b baa7f900 f7c53298 9073cbbd c90690c5 5591553c 43a5d984 af92402d
CV'	791c9c6b baa7f900 f7c53298 9073cbbd c90690c5 5591553c 43a5d984 bf92402d
M	f41d61b4 ce033ba2 dd1bc208 a268189b ee6bda2c 5ddbe94d 9675bbd3 32c1ba8a 7eba797d 88b06a8f 3bc3015c d36f38cc cfcb88e0 3c70f7f3 faa0c1fe 35c62535
M'	e41d61b4 ce033ba2 dd1bc208 a268189b ee6bda2c 5ddbe94d 9675bbd3 32c1ba8a 7eba797d 98b06a8f 39e3055c c36f38cc ce4b002d 3c74f1f3 faa0c1fe 35c62535
hash	9af50cac c165a72f b6f1c9f3 ef54bad9 af0cfb1f 57d357c9 c6462616

Key Research and Development Program of China (No. 2022YFB2701900), the National Natural Science Foundation of China (No. 62072181). Fukang Liu is supported by Grant-in-Aid for Research Activity Start-up (Grant No. 22K21282).

References

1. Aoki, K., Guo, J., Matusiewicz, K., Sasaki, Y., Wang, L.: Preimages for step-reduced SHA-2. In: ASIACRYPT. Lecture Notes in Computer Science, vol. 5912, pp. 578–597. Springer (2009). https://doi.org/10.1007/978-3-642-10366-7_34
2. Biham, E., Chen, R., Joux, A., Carribault, P., Lemuet, C., Jalby, W.: Collisions of SHA-0 and reduced SHA-1. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 3494, pp. 36–57. Springer (2005), https://doi.org/10.1007/11426639_3
3. Biryukov, A., Lamberger, M., Mendel, F., Nikolic, I.: Second-order differential collisions for reduced SHA-256. In: ASIACRYPT. Lecture Notes in Computer Science, vol. 7073, pp. 270–287. Springer (2011). https://doi.org/10.1007/978-3-642-25385-0_15
4. Cannière, C.D., Rechberger, C.: Finding SHA-1 characteristics: General results and applications. In: ASIACRYPT. Lecture Notes in Computer Science, vol. 4284, pp. 1–20. Springer (2006), https://doi.org/10.1007/11935230_1
5. Damgård, I.: A design principle for hash functions. In: CRYPTO. Lecture Notes in Computer Science, vol. 435, pp. 416–427. Springer (1989), https://doi.org/10.1007/0-387-34805-0_39
6. Dobraunig, C., Eichlseder, M., Mendel, F.: Analysis of SHA-512/224 and SHA-512/256. In: ASIACRYPT(2). Lecture Notes in Computer Science, vol. 9453, pp. 612–630. Springer (2015), https://doi.org/10.1007/978-3-662-48800-3_25
7. Draft, F.: Public comments on the draft federal information processing standard (fips) draft fips 180-2, secure hash standard (shs)
8. Eichlseder, M., Mendel, F., Schläffer, M.: Branching heuristics in differential collision search with applications to SHA-512. In: FSE. Lecture Notes in Computer Science, vol. 8540, pp. 473–488. Springer (2014), https://doi.org/10.1007/978-3-662-46706-0_24
9. Guo, J., Ling, S., Rechberger, C., Wang, H.: Advanced meet-in-the-middle preimage attacks: First results on full tiger, and improved results on MD4 and SHA-2. In: ASIACRYPT. Lecture Notes in Computer Science, vol. 6477, pp. 56–75. Springer (2010). https://doi.org/10.1007/978-3-642-17373-8_4
10. Indesteege, S., Mendel, F., Preneel, B., Rechberger, C.: Collisions and other non-random properties for step-reduced SHA-256. In: SAC. Lecture Notes in Computer Science, vol. 5381, pp. 276–293. Springer (2008). https://doi.org/10.1007/978-3-642-04159-4_18
11. Isobe, T., Shibutani, K.: Preimage attacks on reduced tiger and SHA-2. In: FSE. Lecture Notes in Computer Science, vol. 5665, pp. 139–155. Springer (2009). https://doi.org/10.1007/978-3-642-03317-9_9
12. Khovratovich, D., Rechberger, C., Savelieva, A.: Bicliques for preimages: Attacks on skein-512 and the SHA-2 family. In: FSE. Lecture Notes in Computer Science, vol. 7549, pp. 244–263. Springer (2012). https://doi.org/10.1007/978-3-642-34047-5_15
13. Lamberger, M., Mendel, F.: Higher-order differential attack on reduced SHA-256. IACR Cryptol. ePrint Arch. p. 37 (2011), http://eprint.iacr.org/2011/037

14. Landelle, F., Peyrin, T.: Cryptanalysis of full RIPEMD-128. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 7881, pp. 228–244. Springer (2013). https://doi.org/10.1007/978-3-642-38348-9_14
15. Leurent, G., Peyrin, T.: From collisions to chosen-prefix collisions application to full SHA-1. In: EUROCRYPT(3). Lecture Notes in Computer Science, vol. 11478, pp. 527–555. Springer (2019), https://doi.org/10.1007/978-3-030-17659-4_18
16. Leurent, G., Peyrin, T.: SHA-1 is a shambles: First chosen-prefix collision on SHA-1 and application to the PGP web of trust. In: USENIX. pp. 1839–1856. USENIX Association (2020), https://www.usenix.org/conference/usenixsecurity20/presentation/leurent
17. Li, J., Isobe, T., Shibutani, K.: Converting meet-in-the-middle preimage attack into pseudo collision attack: Application to SHA-2. In: FSE. Lecture Notes in Computer Science, vol. 7549, pp. 264–286. Springer (2012). https://doi.org/10.1007/978-3-642-34047-5_16
18. Liu, F., Dobraunig, C., Mendel, F., Isobe, T., Wang, G., Cao, Z.: Efficient collision attack frameworks for RIPEMD-160. In: CRYPTO(2). Lecture Notes in Computer Science, vol. 11693, pp. 117–149. Springer (2019). https://doi.org/10.1007/978-3-030-26951-7_5
19. Liu, F., Dobraunig, C., Mendel, F., Isobe, T., Wang, G., Cao, Z.: New semi-free-start collision attack framework for reduced RIPEMD-160. IACR Trans. Symmetric Cryptol. **2019**(3), 169–192 (2019). https://doi.org/10.13154/tosc.v2019.i3.169-192
20. Liu, F., Isobe, T., Meier, W.: Automatic verification of differential characteristics: Application to reduced gimli. In: CRYPTO. Lecture Notes in Computer Science, vol. 12172, pp. 219–248. Springer (2020). https://doi.org/10.1007/978-3-030-56877-1_8
21. Liu, F., Meier, W., Sarkar, S., Wang, G., Ito, R., Isobe, T.: New cryptanalysis of ZUC-256 initialization using modular differences. IACR Trans. Symmetric Cryptol. **2022**(3), 152–190 (2022), https://doi.org/10.46586/tosc.v2022.i3.152-190
22. Liu, F., Mendel, F., Wang, G.: Collisions and semi-free-start collisions for round-reduced RIPEMD-160. In: ASIACRYPT(1). Lecture Notes in Computer Science, vol. 10624, pp. 158–186. Springer (2017), https://doi.org/10.1007/978-3-319-70694-8_6
23. Liu, F., Wang, G., Sarkar, S., Anand, R., Meier, W., Li, Y., Isobe, T.: Analysis of RIPEMD-160: new collision attacks and finding characteristics with MILP. In: EUROCRYPT(4). Lecture Notes in Computer Science, vol. 14007, pp. 189–219. Springer (2023). https://doi.org/10.1007/978-3-031-30634-1_7
24. Mendel, F., Nad, T., Scherz, S., Schläffer, M.: Differential attacks on reduced RIPEMD-160. In: ISC. Lecture Notes in Computer Science, vol. 7483, pp. 23–38. Springer (2012). https://doi.org/10.1007/978-3-642-33383-5_2
25. Mendel, F., Nad, T., Schläffer, M.: Finding SHA-2 characteristics: Searching through a minefield of contradictions. In: ASIACRYPT. Lecture Notes in Computer Science, vol. 7073, pp. 288–307. Springer (2011), https://doi.org/10.1007/978-3-642-25385-0_16
26. Mendel, F., Nad, T., Schläffer, M.: Collision attacks on the reduced dual-stream hash function RIPEMD-128. In: FSE. Lecture Notes in Computer Science, vol. 7549, pp. 226–243. Springer (2012), https://doi.org/10.1007/978-3-642-34047-5_14
27. Mendel, F., Nad, T., Schläffer, M.: Improving local collisions: New attacks on reduced SHA-256. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 7881, pp. 262–278. Springer (2013), https://doi.org/10.1007/978-3-642-38348-9_16

28. Mendel, F., Peyrin, T., Schläffer, M., Wang, L., Wu, S.: Improved cryptanalysis of reduced RIPEMD-160. In: ASIACRYPT(2). Lecture Notes in Computer Science, vol. 8270, pp. 484–503. Springer (2013). https://doi.org/10.1007/978-3-642-42045-0_25
29. Mendel, F., Pramstaller, N., Rechberger, C., Rijmen, V.: Analysis of step-reduced SHA-256. In: FSE. Lecture Notes in Computer Science, vol. 4047, pp. 126–143. Springer (2006). https://doi.org/10.1007/11799313_9
30. Merkle, R.C.: One way hash functions and DES. In: Brassard, G. (ed.) CRYPTO. Lecture Notes in Computer Science, vol. 435, pp. 428–446. Springer (1989), https://doi.org/10.1007/0-387-34805-0_40
31. Mironov, I., Zhang, L.: Applications of SAT solvers to cryptanalysis of hash functions. In: SAT. Lecture Notes in Computer Science, vol. 4121, pp. 102–115. Springer (2006), https://doi.org/10.1007/11814948_13
32. Nikolic, I., Biryukov, A.: Collisions for step-reduced SHA-256. In: FSE. Lecture Notes in Computer Science, vol. 5086, pp. 1–15. Springer (2008). https://doi.org/10.1007/978-3-540-71039-4_1
33. Sanadhya, S.K., Sarkar, P.: New collision attacks against up to 24-step SHA-2. In: INDOCRYPT. Lecture Notes in Computer Science, vol. 5365, pp. 91–103. Springer (2008). https://doi.org/10.1007/978-3-540-89754-5_8
34. Stevens, M.: New collision attacks on SHA-1 based on optimal joint local-collision analysis. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 7881, pp. 245–261. Springer (2013), https://doi.org/10.1007/978-3-642-38348-9_15
35. Stevens, M., Bursztein, E., Karpman, P., Albertini, A., Markov, Y.: The first collision for full SHA-1. In: CRYPTO(1). Lecture Notes in Computer Science, vol. 10401, pp. 570–596. Springer (2017), https://doi.org/10.1007/978-3-319-63688-7_19
36. Stevens, M., Lenstra, A.K., de Weger, B.: Chosen-prefix collisions for MD5 and colliding X.509 certificates for different identities. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 4515, pp. 1–22. Springer (2007), https://doi.org/10.1007/978-3-540-72540-4_1
37. Wang, X., Lai, X., Feng, D., Chen, H., Yu, X.: Cryptanalysis of the hash functions MD4 and RIPEMD. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 3494, pp. 1–18. Springer (2005), https://doi.org/10.1007/11426639_1
38. Wang, X., Yin, Y.L., Yu, H.: Finding collisions in the full SHA-1. In: CRYPTO. Lecture Notes in Computer Science, vol. 3621, pp. 17–36. Springer (2005), https://doi.org/10.1007/11535218_2
39. Wang, X., Yu, H.: How to break MD5 and other hash functions. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 3494, pp. 19–35. Springer (2005), https://doi.org/10.1007/11426639_2
40. Wang, X., Yu, H., Yin, Y.L.: Efficient collision search attacks on SHA-0. In: CRYPTO. Lecture Notes in Computer Science, vol. 3621, pp. 1–16. Springer (2005), https://doi.org/10.1007/11535218_1
41. Yu, H., Bai, D.: Boomerang attack on step-reduced SHA-512. In: Inscrypt. Lecture Notes in Computer Science, vol. 8957, pp. 329–342. Springer (2014). https://doi.org/10.1007/978-3-319-16745-9_18
42. Yu, H., Wang, X.: Non-randomness of 39-step SHA-256. In: Presented at rump session of EUROCRYPT (2008)

EXHIBIT E

As filed with the Securities and Exchange Commission on February 25, 2021

Registration No. 333-

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, DC 20549

FORM S-1
REGISTRATION STATEMENT
UNDER
THE SECURITIES ACT OF 1933

Coinbase Global, Inc.

(Exact name of registrant as specified in its charter)

Delaware	7389	46-4707224
(State or other jurisdiction of incorporation or organization)	(Primary Standard Industrial Classification Code Number)	(I.R.S. Employer Identification Number)

Brian Armstrong, Chief Executive Officer
Coinbase Global, Inc.
Address Not Applicable[1]
(Address, including zip code, and telephone number, including area code, of registrant's principal executive offices)

The Corporation Trust Company
1209 Orange Street
Wilmington, Delaware 19801
(302) 777-0200
(Name, address, including zip code, and telephone number, including area code, of agent for service)

Mark C. Stevens
Michael A. Brown
Ran D. Ben-Tzur
Faisal Rashid
Jennifer J. Hitchcock
Fenwick & West LLP
228 Santa Monica Blvd, Suite 300
Santa Monica, California 90401
(310) 434-5400

Copies to:

Paul Grewal
Juan Suarez
Doug Sharp
Coinbase Global, Inc.
Address Not Applicable[1]

Satoshi Nakamoto
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

Approximate date of commencement of proposed sale to the public:
As soon as practicable after this registration statement becomes effective.

If any of the securities being registered on this Form are to be offered on a delayed or continuous basis pursuant to Rule 415 under the Securities Act of 1933, as amended, or Securities Act, check the following box: ☒

If this Form is filed to register additional securities for an offering pursuant to Rule 462(b) under the Securities Act, please check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

If this Form is a post-effective amendment filed pursuant to Rule 462(c) under the Securities Act, check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

If this Form is a post-effective amendment filed pursuant to Rule 462(d) under the Securities Act, check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

[1] In May 2020, we became a remote-first company. Accordingly, we do not maintain a headquarters.

EXHIBIT F

CLASSIFICATION GUIDE TITLE/NUMBER: (U//FOUO) PROJECT BULLRUN/2-16

PUBLICATION DATE: 16 June 2010

OFFICE OF ORIGIN: (U) Cryptanalysis and Exploitation Services

POC: (U) Cryptanalysis and Exploitation Services (CES) Classification Advisory Officer

PHONE: [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: [redacted]

1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE, interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques. Several ECIs apply to the specific sources, methods, and techniques involved. Because of the multiple sources involved in BULLRUN activities, "capabilities against a technology" does not necessarily equate to decryption.

2. (U//FOUO) The BULLRUN data label (for use in databases) and marking (for use in hard- or softcopy documents) are for internal NSA/CSS use only. It will appear in the classification line and corresponding portion markings after all applicable ODNI-approved markings are in place. The format is:
Classification//SCI Control System Markings//CAPCO-approved Dissemination Control Markings/BULLRUN. Examples include:

- TOP SECRET//SI//REL TO USA, FVEY/BULLRUN
- TOP SECRET//SI-ECI PIQ//ORCON/NOFORN/BULLRUN

3. (U//FOUO) Appendix A lists specific BULLRUN capabilities. Details may be protected by one or more ECI. Contact CES CAO for access to the appendix or further guidance.

Description of Information	Classification/Markings	Reason	Declass	Remarks
A. (U) General				
A.1. (U) The coverterm BULLRUN standing alone	UNCLASSIFIED	N/A	N/A	
A.2. (U//FOUO) The coverterm BULLRUN in association with	UNCLASSIFIED// FOR OFFICIAL USE ONLY	N/A	N/A	(U//FOUO) Related ECIs include, but are not limited to:

Description of Information	Classification/Markings	Reason	Declass	Remarks
NSA/CSS, SIGINT, IC, or any of the related ECIs				APERIODIC, AMBULANT, AUNTIE, PAINTEDEAGLE, PAWLEYS, PITCHFORD, PENDLETON, PICARESQUE, PIEDMONT
B. (U) Partnering/Collaboration				
B.1. (U) The fact that Cryptanalysis and Exploitation Services (CES) works with: • NSA/CSS Commercial Solutions Center (NCSC) • Tailored Access Operations (TAO) • Second Party partners	UNCLASSIFIED	N/A	N/A	
B.2. (U//FOUO) The fact that Cryptanalysis and Exploitation Services (CES) works with: • NSA/CSS Commercial Solutions Center (NCSC) to leverage sensitive, cooperative relationships with specific industry partners • Tailored Access Operations (TAO) to leverage specific computer network exploitation activities • specific U.S. Government/IC entities to further NSA/CSS capabilities against encryption used in network communication technologies	TOP SECRET//SI// REL TO USA, FVEY See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
B.3. (TS//SI//REL) Details of the CES collaboration with: • NSA/CSS Commercial Solutions Center (NCSC) to leverage sensitive, cooperative relationships with industry partners • Tailored Access Operations (TAO) to leverage computer network exploitation activities • Second Party partners • specific U.S. Government/IC entities to further NSA/CSS capabilities against encryption used in network communication technologies	TOP SECRET//SI// REL TO USA, FVEY at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.

Description of Information	Classification/Markings	Reason	Declass	Remarks
C. (U) Capabilities & Targeting				
C.1. (U//FOUO) The fact that Cryptanalysis and Exploitation Services (CES) develops cryptanalytic capabilities to exploit the inherent vulnerabilities in the encryption used in unspecified network communication technologies	UNCLASSIFIED// FOR OFFICIAL USE ONLY	N/A	N/A	
C.2. (U//FOUO) The fact that NSA/CSS targets specific encrypted network communication technologies	SECRET//SI// REL TO USA, FVEY at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details may raise classification level and may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
C.3. (TS//SI//REL) The fact that NSA/CSS has some capabilities against the encryption in TLS/SSL, HTTPS, SSH, VPNs, VoIP, WEBMAIL, and other network communication technologies	TOP SECRET//SI// REL TO USA, FVEY at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
C.4. (U//FOUO) The fact that NSA/CSS has a capability against the encryption used in a specific implementation of a network communication technology	TOP SECRET//SI// REL TO USA, FVEY/ BULLRUN at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Specific implementations may be identified by specifying equipment manufacturer, service provider or target implementation. (U//FOUO) Details may be protected by one or more ECIs

Description of Information	Classification/Markings	Reason	Declass	Remarks
				and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
C.5. (U//FOUO) Details revealing specific sources and methods that enable a capability against the encryption used in network communication technologies	TOP SECRET//SI// REL TO USA, FVEY at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
C.6. (TS//SI//REL TO USA, FVEY) The fact that NSA/CSS develops implants to enable a capability against the encryption used in network communication technologies	TOP SECRET//SI// REL TO USA, FVEY See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details will be protected by one or more ECIs. Contact CES CAO for further guidance.
D. (U) Processing & Handling				
D.1. (U//FOUO) Decrypts (aka plaintext) obtained from BULLRUN capabilities	TOP SECRET//SI// REL TO USA, FVEY/ BULLRUN at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Decrypts or any data extracted from the decrypts must be handled within the secure BULLRUN COI and must be marked with the BULLRUN data label, unless Chief S31 (or designee) has approved handling or dissemination outside of BULLRUN. Reports generated from BULLRUN-derived information must not reveal BULLRUN details. (U//FOUO) Details may be

Description of Information	Classification/Markings	Reason	Declass	Remarks
				protected by one or more ECIs. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
D.2. (U//FOUO) Cryptographic information obtained from BULLRUN capabilities	TOP SECRET//SI// REL TO USA, FVEY/ BULLRUN at a minimum See Remarks.	1.4 (c)	25 years*	(U) Examples include algorithm parameters and passwords. (U//FOUO) Details may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.

(U) 25 years*: Declassification in 25 years indicates that the information is classified for 25 years from the date a document is created or 25 years from the date of this original classification decision, whichever is later.

(U) ACRONYMS/DEFINITIONS:

(U) **Capabilities** – For the purposes of this classification guide, the NSA/CSS ability to exploit a specific technology. This may encompass acquiring and processing plaintext data and/or acquiring, decrypting and processing encrypted data.

(U) **HTTPS** – HTTP traffic secured inside an SSL/TLS session, indicated by the https:// URL, commonly using TCP port 443

(U) **IPSEC -- IPSec**, or **IP Security**, is the Internet Engineering Task Force (IETF) standard for layer 3 real-time communication security. IPSec allows two hosts (or two gateways) to establish a secure connection, sometimes called a tunnel. All traffic is protected at the network layer. (IETF is the Internet Engineering Task Force, a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies. It is the principal body engaged in the development of new Internet standard specifications.)

(U) **PPTP – Point-to-Point Tunneling Protocol** is a method for implementing virtual private networks. The PPTP specification does not describe encryption or authentication features and relies on the protocol being tunneled to implement security functionality.

(U) **SSH – Secure Shell.** A common protocol used for secure remote computer access

(U) **SSL – Secure Sockets Layer.** Commonly used to provide secure network communication. Widely used on the internet to provide secure web browsing, webmail, instant messaging, electronic commerce, etc.

(U) **TLS – Transport Layer Security.** The follow-on to SSL, SSLv3 and TLSv1.0 are nearly identical.

(U) **VoIP – Voice over Internet Protocol.** A general term for the using IP networks to make voice phone calls. The application layer protocol can be standards-based (e.g., H.323, SIP), or proprietary (e.g., Skype).

(U) **VPN – Virtual Private Network.** A private network that makes use of the public telecommunications infrastructure, maintaining privacy via the use of a tunneling protocol and security procedures that typically include encryption. Common protocols include IPSEC and PPTP.