The Case Against Bitcoin

By: Marc Fitapelli, Esq.
www.mdf-law.com

Abstract

Individuals who invest in Bitcoin blindly place their trust in an anonymous individual they do not know and a technology they do not understand. The US dollar says, "In God we trust," because Americans trust only God blindly. Every participant in America's brand of free market capitalism is untrusted and subject to public checks and balances. Everyone in our free-market democracy must publicly answer to government regulators, except Satoshi Nakamoto.[1] Bitcoin has no utility and is merely spreadsheet money. Bitcoin is not a currency and still cannot be used to buy goods and services. It is a poor investment because it trades in a manipulated market. Bitcoin will eventually go to zero.

1. Bitcoin is an investment, but that is 'dangerous to say' according to Satoshi Nakamoto's private emails.

The Bitcoin Creator invented Bitcoin to be used as a currency. This use case failed many years ago. Bitcoin cannot be used to buy goods and services. Instead of acting as currency, Bitcoin has evolved into a 'store of value,' which is often compared to physical gold. People invest in Bitcoin because they hope to make money in the future. The federal government does not regulate Bitcoin like other investments. Bitcoin is not regulated like stocks, bonds and mutual funds. This is because Bitcoin is not considered a "security" under the *Howey*-test.[2] This means Bitcoin investors do not receive any protections from the Securities and Exchange Commission. This is bad for consumers, but good for Wall Street and Silicon Valley. The decision to categorize Bitcoin as a "non-security" (known as the "Bitcoin Loophole") was not made by Congress or even judges. It was made by a political appointee, who is as anonymous to America as Satoshi Nakamoto.

[1] The "Bitcoin Creator" shall mean Satoshi Nakamoto, the alleged inventor of Bitcoin. This author will use the pronouns he/him to refer to the "Bitcoin Creator," or "Satoshi Nakamoto." Readers should not conclude that the Bitcoin Creator is a man because of these pronouns. He could be a group of people or even a sovereign government.

[2] The "Howey Test" means the test the United States Supreme Court created in 1946 to help interpret the Securities and Exchange Act of 1934. *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). The test is used to determine if new, complex, financial instruments should be regulated. The Securities and Exchange Commission should not be responsible for interpreting *Howey* – only Congress and Courts should have this authority.

2. Banks are better than Bitcoin.

The banking system is better than Bitcoin. The banking system has multiple consumer safeguards that prevent fraud. First, there are no anonymous users in the banking system and every market participant's identity is known to at least one trusted third party (i.e. the bank). The banking system trusts, but verifies. Because of this safeguard, it is difficult for a criminal to clandestinely open a bank account. Second, banking transactions, unlike blockchain transactions, can be reversed for fraud. In addition to being reversable, there are also state and Federal laws, which shift fraud losses from negligent consumers to banks. Cryptocurrency investors have no similar protections.

Here is a graphical representation of why normal banks are better than Bitcoin:

Banking System (USD)	The Blockchain (Bitcoin)
➢ More Democratic. A system with checks and balances. It trusts, but also verifies so all market participants are treated equally under the law.	➢ Less Democratic. A system with blind trust in technology. Participants with more resources can cheat other market participants.
➢ Consumer Friendly. Transactions are reversable for fraud.	➢ Buyer Beware. Transactions are never reversable, even for fraud.
➢ KYC. Difficult for criminals to open accounts because you cannot own a bank account without providing KYC information.	➢ Non-KYC. Fast and easy for criminals to open accounts. Criminals do not need to provide KYC information to own Bitcoin.
➢ Trusted Third Party. Banks verify the integrity of the system and prevent criminals from opening back accounts. Banks are legally and financially incentivized to prevent fraud.	➢ Untrusted Third Party. Miners do difficult math problems to verify the integrity of the system. Bitcoin miners do not care if Bitcoin investors are defrauded.

Both Bitcoin and the US Dollar need third parties for their respective systems to work. Banks are "Trusted Third Parties" because they are legally and financially incentivized to prevent fraud. In exchange for providing banks with KYC information, customers are provided with insurance against fraud and other bad acts. If banks do a poor job of preventing fraud, they will be shut down. This is how the banking system efficiently eliminates fraud. It is called self-regulation. Self-regulation works because its members are incentivized by the constant threat of government regulators. America does not regulate Bitcoin. Therefore, the Bitcoin industry does not have a legal incentive to prevent fraud. Bitcoin uses "Untrusted Third Parties." These parties are known

as "miners." These parties are incentivized to calculate a math problem quickly. The risk of fraud in the Bitcoin industry will always be on the consumer under this type of system.

> **Mark Cuban (2023).** In September 2023, Mark Cuban was hacked and approximately $1 million in cryptocurrency was stolen from his KYC Wallet. [3] If the hack occurred in a bank account, the bank would have been required by law to reimburse the full amount stolen, even above FDIC limits.[4]

3. Satoshi Nakamoto is violating the US Patriot Act and Bank Secrecy Act.

After September 1, 2001, Americans stopped living in a free world. If we want to be "free," we must trust a third party with more resources to protect us from bad actors. Our post 9/11 financial system protects us because it uses "trusted third parties," known as banks. If you invest in Bitcoin, you are investing in a system that uses blind trust. The lesson from September 11, 2001, was trust, but verify. Individuals who invest in Bitcoin trust, but do not verify. Bitcoin has no system of checks and balances, which makes it inherently unsafe.

After 9/11, our government passed the United States Patriot Act. This law was designed to prevent future terrorist attacks by eliminating dirty money from our financial system. As a result, every single American who opens a Bitcoin wallet must provide their exchange with their driver's license and social security number.[5] With few exceptions, all American users of cryptocurrency are not anonymous, and their identities can be ascertained through a subpoena. These Americans all own "KYC Wallets." [6]

Criminals create true anonymous wallets (known as "Non-KYC Wallets") to steal cryptocurrency and commit other crimes, including state sponsored terrorism. Non-KYC Wallets are modern Swiss bank accounts, but easier to attain. The presence of Non-KYC Wallets makes Bitcoin a pseudo-anonymous system and not a true-anonymous system. Most "true anonymous" Bitcoin

---

[3] https://www.coindesk.com/tech/2023/09/18/mark-cuban-loses-nearly-1m-to-crypto-scam/

[4] Here is a video of the CEO of JP Morgan Chase Bank, Jamie Dimon, discussing the law before a senate banking committee meeting: https://www.youtube.com/watch?v=Nkfud0swVzw.

[5] This is known as "know your customer," or KYC information. All American users of Bitcoin complete KYC information and therefore have "KYC Wallets."

For more information about KYC: https://en.wikipedia.org/wiki/Know_your_customer

[6] "KYC Wallets" means any wallet that is owned by someone who provided KYC information to a trusted third party.

users are physically located in North Korea[7], Russia,[8] the Middle East[9] and China.[10] These users also operate in the United States by using Virtual, Private Networks, or VPNs. These illegal users of Bitcoin, including the Bitcoin Creator, are increasingly exploiting the Bitcoin Loophole to harm honest Americans.

4. Satoshi Nakamoto is violating the Securities and Exchange Act.

Satoshi Nakamoto was careful not to use the phrase "consider it an investment" on Bitcoin's first website. He thought it would be a "dangerous thing to say." Here is his email:

> 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.

Satoshi Nakamoto to European Bitcoin developer, Martii Malmi, June 11, 2009[11]

If Bitcoin were a stock, its founder's identity would be publicly disclosed in filings with the Securities and Exchange Commission. To date, the identity of Bitcoin's founder and the author of its famous whitepaper are unknown to the public. Satoshi Nakamoto may be an individual or group of individuals. If he was a person, he would be among the 20 richest individuals in the

[7] North Korea crypto hacking activity soars to record high in 2023, new report shows (cnbc.com) https://www.cnbc.com/2024/01/24/north-korea-crypto-hacking-activity-soars-to-record-high-in-2023-new-report-shows.html

[8] Russian regulator encourages use of crypto to counter sanctions (Reuters, July 3, 2024) https://www.reuters.com/business/finance/russian-regulator-encourages-use-crypto-counter-sanctions-2024-07-03/

[9] The Middle East is pitching itself as the future of crypto. Will companies follow? - Fortune https://fortune.com/crypto/2024/03/06/dubai-crypto-saudi-vara-blockchain-regulation-mena-middle-east/

[10] Across U.S., Chinese Bitcoin Mines Draw National Security Scrutiny - The New York Times https://www.nytimes.com/2023/10/13/us/bitcoin-mines-china-united-states.html

[11] This email is from a series of emails disclosed to the public in 2024 by a man named Martti Malami, an early developer of Bitcoin. The native file has not been reviewed by the author, but this email is believed to be genuine. The context of the email is described in the preceding paragraphs. All of the emails between "Satoshi" and Mr. Malami can be accessed here: https://mmalmi.github.io/satoshi/

world because he is believed to have amassed at least 1 million Bitcoin in the year 2009 alone.[12] As a result, the Bitcoin Creator is believed to be worth between $50 - $100 billion US Dollars.

In June 2009, the Bitcoin Creator asked a European man named, Martti Malami, to establish Bitcoin's first website. The Bitcoin Creator did not want to pay the hosting fees for the website because he was concerned his identity could be disclosed through a lawfully issued subpoena in the United States. To evade U.S. laws, including the United States Patriot Act, the Bitcoin Creator asked another anonymous investor to mail currency, US Dollars, to Europe and directed Mr. Malami to 'keep the envelope's origin private.' This is how Bitcoin's first website was established.

Satoshi Nakamoto was especially sensitive about referring to Bitcoin as an 'investment.' Here are portions of a 2009 email where he discussed outside investors: "[t]here 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."

America is wrong to romanticize Satoshi Nakamoto.

The Bitcoin market will never be efficient if its largest market participant continues to remain anonymous. The Bitcoin Creator is dangerous to free market capitalism. He can liquidate all his Bitcoin and crash Bitcoin as well as the securities markets without any legal consequences.

5. Hack Bitcoin once, shame on Bitcoin, hack Bitcoin twice, shame on Bitcoin investors.

Bitcoin uses cryptography to secure a peer-to-peer network where pseudo-anonymous users can transfer tokens to each other. Once tokens are transferred, the transactions are recorded on a type of spreadsheet that can never be changed. Bitcoin's purported appeal is that it can be verified without the need for a centralized, trusted third party, such as a bank or government. Instead, Bitcoin uses decentralized computers as untrusted third parties. These "Miners" utilize expensive hardware to guess the answer to a math problem, which verifies Bitcoin's spreadsheets so that users do not spend more tokens than 21 million. It is very similar to a race to compute *Pi* to the largest decimal point. The computer who comes closest to the answer earns chances to be rewarded with new Bitcoin.

It is computationally impossible for a computer to "hack" Bitcoin through brute force. It is foolish to assume other means will not be successful.[13] It is not a question of if, but when a "Bitcoin Collision" will occur. When this event occurs, the entire Bitcoin market will implode because everyone will lose faith in Bitcoin's code.

Bitcoin is supposed to have a cap of 21 million tokens, but that cap can be hacked.

> Value Overflow Incident of 2010: The first incident occurred in 2010 when an unknown hacker was able to generate 184 billion Bitcoins. The incident exposed a bug that would

[12] See description here: https://blog.bitmex.com/satoshis-1-million-bitcoin/

[13] Google Online Security Blog: Announcing the first SHA1 collision (googleblog.com) https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

have allowed a remote hacker to bypass the 21 million limit and create more Bitcoins.[14] The bug was thought to be fixed in 2010. It was not.

Value Overflow Incident of 2018: In 2018, the bug resurfaced in a more serious, but less widely publicized incident.[15] The 2018 incident was kept secret by Bitcoin's developers so it could be fixed before altering the general public.[16]

The value overflow incidents exposed rudimentary mistakes made in the coding of Bitcoin. Bitcoin was created in 2008-2009 using a programing language called C++.[17] Since its release in 2009, the size of Bitcoin's code has more than tripled. The changes are made by individuals other than the Bitcoin Creator, some of these individuals are anonymous foreign nationals. The code constantly needs updating because Bitcoin's original code was incomplete and contained numerous errors.

6. Satoshi, Gary Gensler and even Jeff Bezos were hacked.

Bitcoin uses a type of encryption called secure hash algorithm, or SHA.[18] This encryption was designed by the United States National Security Administration, or NSA, in the late 1990s and released to the public in 2002. In 2013, Edward Snowden leaked documents about the program, which was codenamed "project Bullrun" after the famous Civil War Battle of Bullrun.[19] "Project

[14] This notice describes the technical details of the attack as well as the fix, which was applied in 2010. https://www.cve.org/CVERecord?id=CVE-2010-5139

[15] This notice describes the same thing, except it pertains to the second attack in 2018. https://bitcoincore.org/en/2018/09/20/notice/

[16] The Latest Bitcoin Bug Was So Bad, Developers Kept Its Full Details a Secret - CoinDesk https://www.coindesk.com/markets/2018/09/21/the-latest-bitcoin-bug-was-so-bad-developers-kept-its-full-details-a-secret/

[17] Random numbers can only be generated using an analog computer. Bitcoin was created using the 'rand()' function in C++. This function is not considered secure. Mersenne Twister 'mt19937' was incorporated into a 2011 update to C++. Mersenne Twister is also not cryptologically secure, but more secure than 'rand()'. Both of functions are known as "pseudo-random number generator" functions or PRNG. The PRNGs are called "pseudo" because digital computers cannot generate true random numbers.

[18] SHA was created by the United States National Security Agency and released to the public on February 1, 2003. See this notice: https://www.federalregister.gov/documents/2002/08/26/02-21599/announcing-approval-of-federal-information-processing-standard-fips-180-2-secure-hash-standard-a

[19] Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security (ProPublica): https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption

Bullrun" was a clandestine, highly classified program to crack internet encryption technology by inserting a type of backdoor into the code.[20] Because of project Bullrun, and other clandestine decryption operations, everyone is subject to hacking, even hacking by foreign governments.

As a result, even Saudia Arabia has a 'backdoor' to Bitcoin, but also everything else on the internet.

> **Satoshi Nakamoto (2014).** In 2014, the email address used by Satoshi, satoshin@gmx.com, was hacked.[21] During the attack, a hacker was able to send messages to reporters and other members of the Bitcoin community. The hacker also verified they were able to access all of "Satoshi's" emails from 2008-2009.
>
> **Jeff Bezos (2020).** In 2020, Jeff Bezos was hacked.[22] He was targeted because his newspaper was critical of Suadi Arabia. [23] Bitcoin helps facilitate these types of crimes.
>
> **Gary Gensler (2024).** In 2024, the SEC was SIM swapped. The hacker posted about Bitcoin using Google Gary's official government handle. [24] By posing as Google Gary, the hacker was able to manipulate the stock market to make substantial sums of money.

7. Conclusion.

Satoshi Nakamoto said it would be "dangerous" to tell consumers Bitcoin was an investment. This author believes well-informed people should be allowed to invest in Bitcoin. You should make your own conclusions about Bitcoin, Satoshi Nakamoto and Gary Gensler.

---

[20] https://en.wikipedia.org/wiki/Bullrun_(decryption_program)

[21] Bitcoin Creator Satoshi Nakamoto Has Lost Control Of His Email Address - Forbes
https://www.forbes.com/sites/kashmirhill/2014/09/08/bitcoin-creator-satoshi-nakamoto-email/

[22] How the Saudis hacked Jeff Bezos' phone, and how to protect yourself (cnbc.com)
https://www.cnbc.com/2020/01/22/how-the-saudis-hacked-jeff-bezos-phone-and-how-to-protect-yourself.html

[23] Jeff Bezos phone hacking incident - Wikipedia
https://en.wikipedia.org/wiki/Jeff_Bezos_phone_hacking_incident

[24] New details emerge about SEC's X account hack, including SIM swap
https://www.cnbc.com/2024/01/22/new-details-emerge-about-secs-x-account-hack-including-sim-swap.html