FACTS MA

FOSTERING ADVOCACY AND COLLABORATION THROUGH SCIENCE

Risks and other Downsides of Blockchain Technology

COMMITTEES

House Energy and Commerce Committee; Science, Space, and Technology Committee

Senate Commerce, Science, and Transportation Committee; Committee on Finance

For further information contact FACTS•MA
contact@factsma.org

Follow us @FACTS-MA

www.factsma.org

Blockchain technology allows a secure, unforgeable public record of transactions, financial (i.e. Bitcoin) or otherwise (i.e. land titles)[1,2,3]. It is useful when parties want records that all parties can access, but that no party can change without authorization. However, blockchain technology poses a number of risks and downsides.

Speculation and Price Volatility in Cryptocurrencies

- A majority of bitcoins are used for speculation, not to buy goods, leading to price volatility characteristic of high-risk commodities[4].
  - Such volatility undermines Bitcoin's use as a currency.

Human Error

- Blockchain applications are vulnerable to errors in the code that implements them, fraudulent use, and theft of passwords[5,6].
  - The open-access nature of blockchain networks makes it hard for malicious code to be inserted, but it does not prevent exploitation of bugs or attacks targeting individuals.

Lack of Regulation of Cryptocurrency Transactions and Infrastructure

- Lack of consumer protection exposes individuals to fraud risk.
  - Bitcoin transfers are irrevocable, with no dispute resolution.
- Lack of financial oversight exposes institutions to bankruptcy risk.

Facilitation of Criminal Activity

- The lack of government oversight facilitates criminal transactions[15].
- Black-market sites can move bitcoin across borders[15].
- Nonetheless, many cryptocurrency crimes are solved[16].

Uncertain Delegation of Authority

- For non-financial blockchain applications, it is unclear who delegates authority to claim ownership of items, such as deeds or votes.
  - If this power falls to a government or other trusted third party, the advantage over a standard secure database is unclear[7].

Network Domination

- If more than 50% of a network conspires, it can manipulate blocks to its advantage (e.g., take back bitcoins it had already spent)[17].
  - Domination of a financial network, such as Bitcoin, is impractical, as it would cost more than the bitcoins that could be stolen[8,9].
  - State-sponsored cryptocurrencies are dominated by the state[10].

Lack of Appropriate Incentives for Non-Financial Blockchains

- For cryptocurrencies, network participation is rewarded financially, so it is more profitable to cooperate than to attack the network[9].
  - For other applications (such as voting), the value of attacking the network might be greater than the cost of the attack.
  - Having a government provide an indomitable network requires that it be trusted, undermining the advantage of a blockchain.

Inappropriate Application of Blockchain Technology

- Blockchain technology is an elegant and powerful solution to the problem of trusted, public record keeping, but it is not magic.
  - It provides nothing beyond secure, public record keeping[7].

Updated February 11, 2018

Sources

[1] "Blockchain Technology". FACTS•MA, 11 February 2018
https://www.factsma.org/factsheets/blockchain-technology

[2] "The Applications of Blockchain Technology". FACTS•MA, 11 February 2018
https://www.factsma.org/factsheets/blockchain-applications

[3] "Blockchains: The great chain of being sure about things". The Economist, 31 October 2015
https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

[4] "Investing in Cryptocurrency: Do or Don't?". Mark Williams, BU Today, 30 January 2018
https://www.bu.edu/today/2018/investing-in-cryptocurrency

[5] "Cryptocurrency Worth $530 Million Missing From Japanese Exchange". Takashi Mochizuki and Paul Vigna, The Wall Street Journal, 26 January 2018
https://www.wsj.com/articles/cryptocurrency-worth-530-million-missing-from-japanese-exchange-1516988190

[6] "How Bitcoin Is Stolen: 5 Common Threats". Jeff John Roberts, Fortune, 8 December 2017
http://fortune.com/2017/12/08/bitcoin-theft

[7] "Blockchain: Almost Everything You Read Is Wrong". Steve Wilson, Constellation Research, 3 May 2016
https://www.constellationr.com/blog-news/blockchain-almost-everything-you-read-wrong

[8] "How Safe Are Blockchains?". Allison Berke, Harvard Business Review, 7 March 2017
https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

[9] "How banks or governments could wipe Bitcoin off the face of the planet". Lexie, ExpressVPN, 18 August 2017
https://www.expressvpn.com/blog/how-to-destroy-bitcoin

[10] "State-sponsored cryptocurrency". Eric Piscini, Deloitte, 2015
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/strategy/us-cons-state-sponsored-cryptocurrency.pdf

[11] "Bitcoin's insane energy consumption, explained". Timothy B. Lee, Ars Technica, 6 December 2017
https://arstechnica.com/tech-policy/2017/12/bitcoins-insane-energy-consumption-explained

[12] "Proof of Work vs Proof of Stake". Blockgeeks
https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake

[13] "Quantum Computers Pose Imminent Threat to Bitcoin Security". MIT Technology Review, 8 November 2017
https://www.technologyreview.com/s/609408/quantum-computers-pose-imminent-threat-to-bitcoin-security

[14] "Quantum Public-Key Cryptosystems". Tatsuaki Okamoto *et al*, Advances in Cryptology – CRYPTO 2000, p. 147, 20 August 2000
https://www.iacr.org/archive/crypto2000/18800147/18800147.pdf

[15] "The Dark Side of Bitcoin: Illegal Activities, Fraud, and Bitcoin". Frederick Coleman, Bloconomics, 16 June 2017
https://blog.blockonomics.co/the-dark-side-of-bitcoin-illegal-activities-fraud-and-bitcoin-360e83408a32

[16] "Why criminals can't hide behind Bitcoin". John Bohannon, Science, 9 Mar.ch 2016
http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

[17] "Bitcoin is 100x less secure than commonly believed". Daniel Larimer, 29 September 2015
http://bytemaster.github.io/update/2015/09/29/Bitcoin-is-100x-less-secure-than-commonly-believed