Evaluating User Privacy in Bitcoin

Alexandra Fuiks '14
Wellesley College

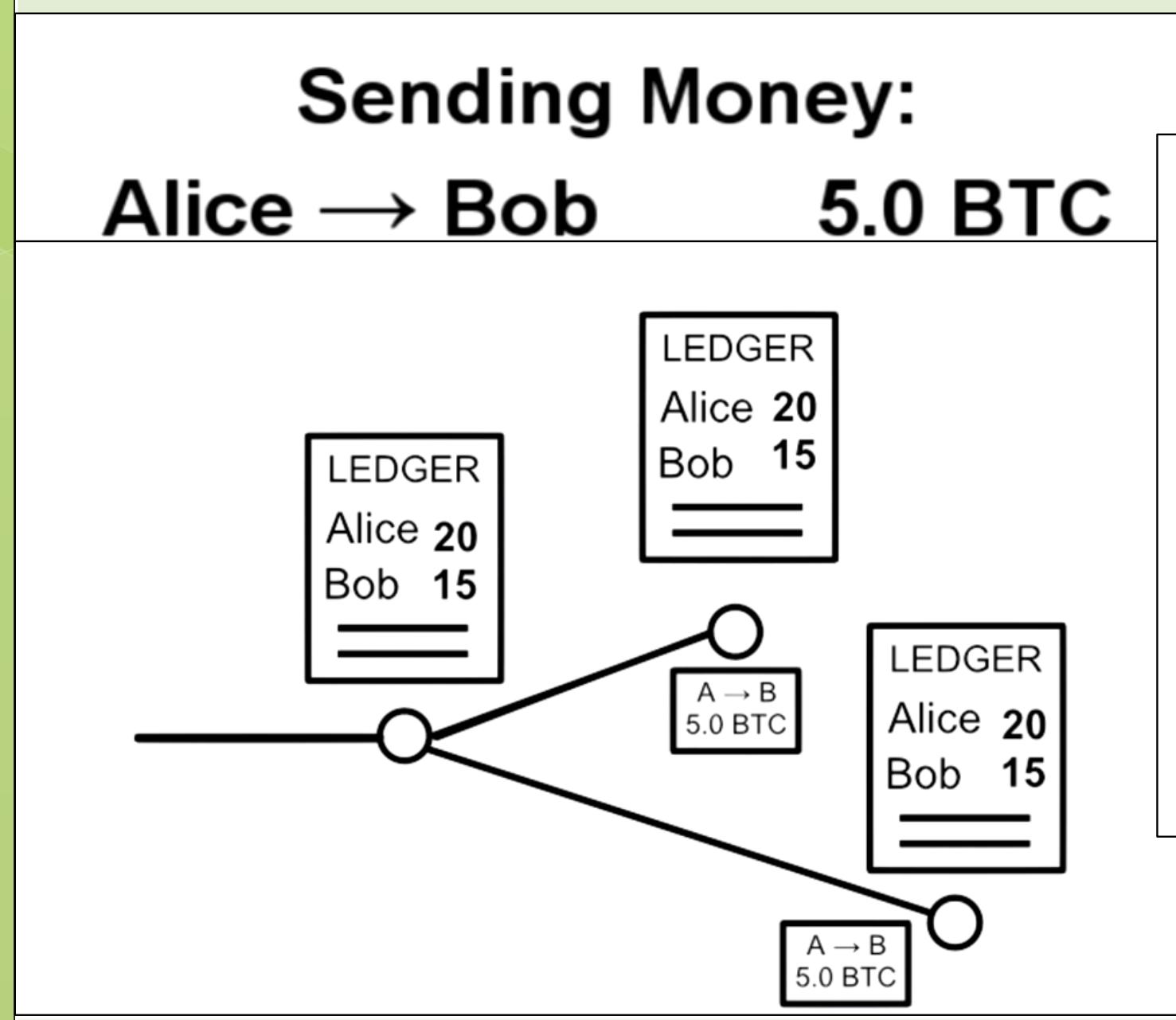
Advisor: Professor Ellen Hildreth
Computer Science

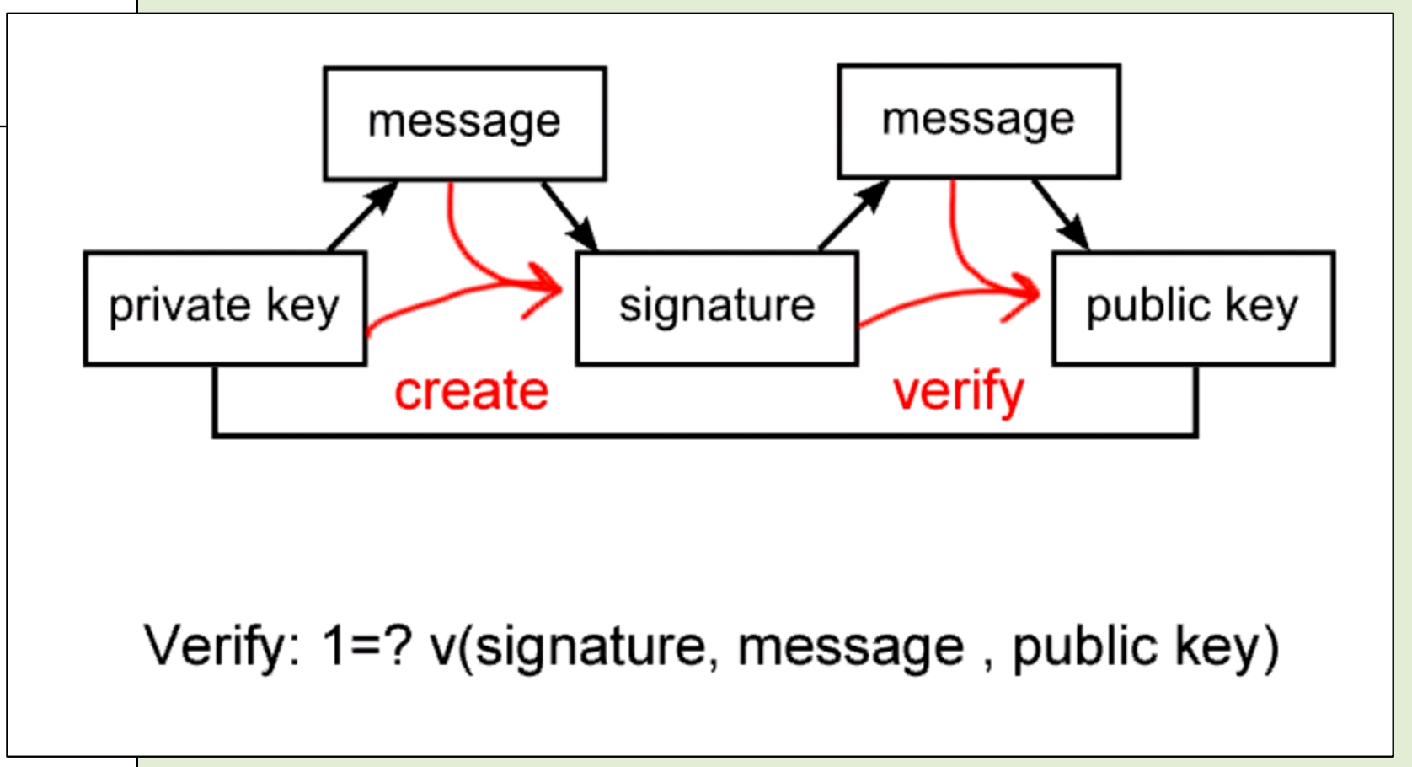
Introduction

For the past half-century, futurists have heralded the advent of a cash-less society. Many of their predictions have been realized, e.g. the "on-line real-time" payment system and bank-maintained central information files. However, cash is still a competitive and relatively anonymous means of payment. Bitcoin is an electronic analog of cash in the online world. It is decentralized, meaning that there is no central authority responsible for the issuance of Bitcoins and there is no need to involve a trusted third-party when making online transfers. However, this flexibility comes at a price: the entire history of Bitcoin transactions is publicly available and attacks by colluding groups seeking monetary gain can put users at risk. In my project, I analyze the structure of the Bitcoin system, in particular its economic implications for user privacy and anonymity.

The Basics of Bitcoin

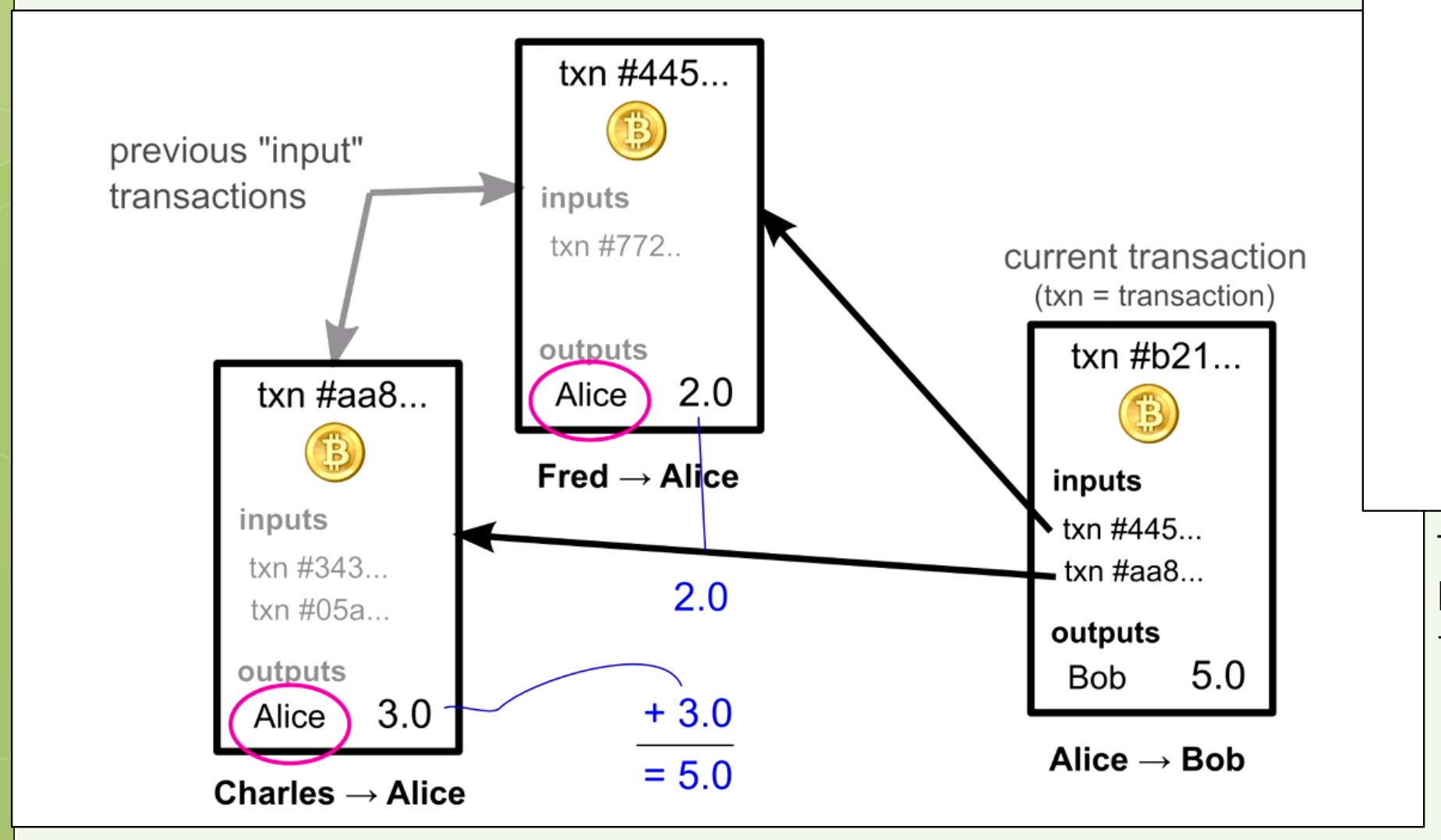
Bitcoin is a an electronic currency that has recently emerged as a popular medium of exchange, with a rich and extensive ecosystem. The Bitcoin network runs at over $40*10^{18}$ FLOPS, with a total market capitalization of approximately 1.5 billion US Dollars as of October 2013. Below is an illustrative map of how a standard transaction occurs. In the following transaction, Alice wishes to send Bob five Bitcoins.



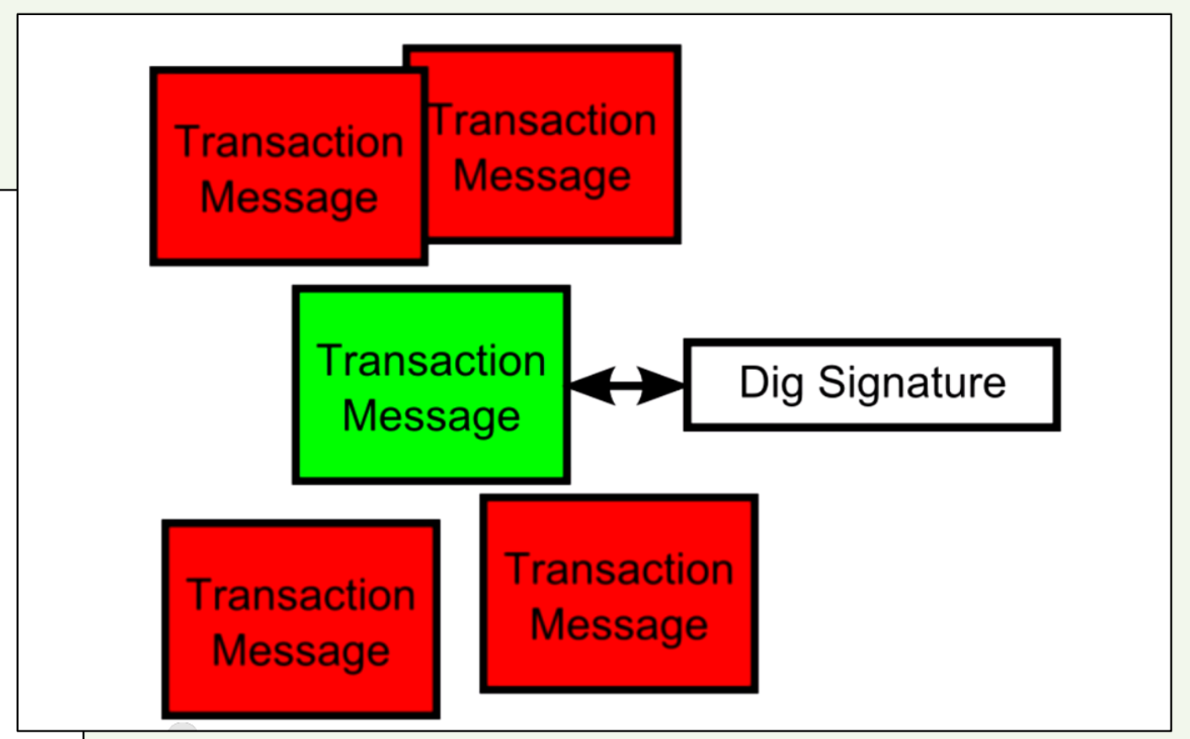


Public keys are the send-to addresses in Bitcoin. To spend money, you must prove that you are the owner of a public key where money was sent. Bitcoin's mathematical component allows this to be done without actually seeing the public keys explicitly.

Generate digital signature from a transaction message and a user's private key to confirm transaction. Other nodes then use this signature to verify that it corresponds with your public key.



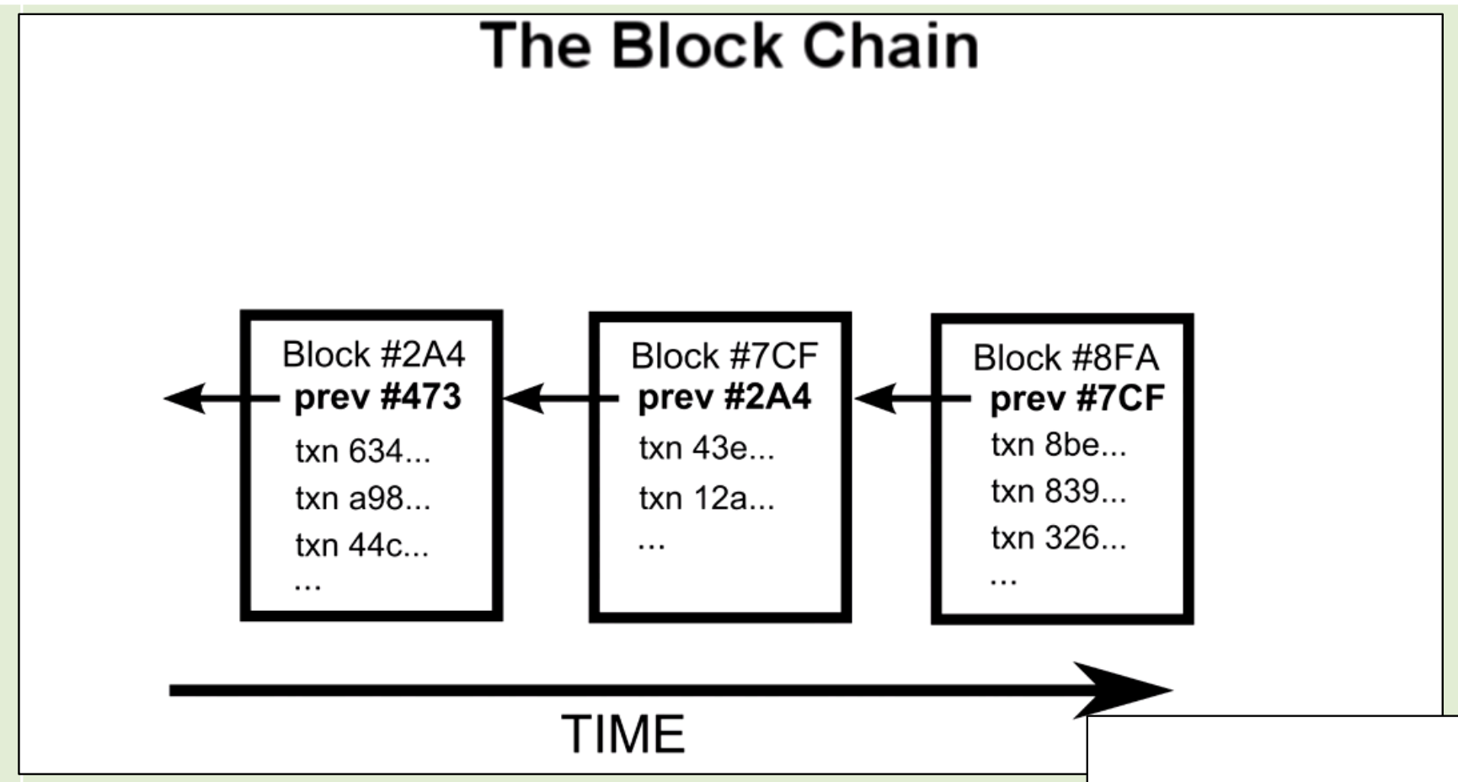
Ownership of funds is verified via links to previous transactions. To send 5 Bitcoins to Bob, Alice must reference 5 or more transactions where she received 5 Bitcoins. These reference transactions are called inputs. Other nodes verifying these inputs will check these transactions to ensure that Alice was the recipient and that the inputs add up to 5 or more Bitcoins.



The signature depends on the message, so it will be different for every transaction. Any changes to the signature will invalidate it.

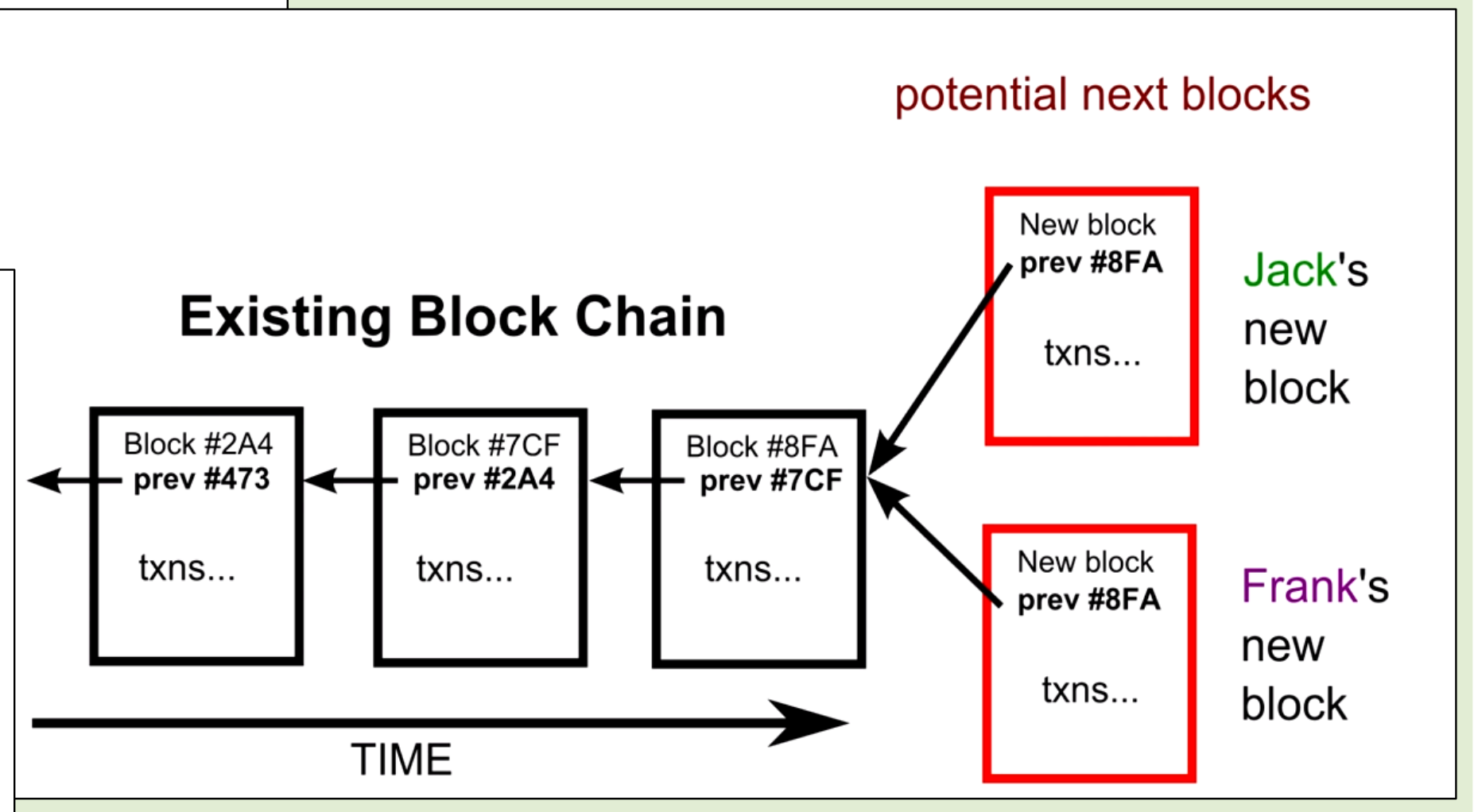
Bitcoin's Mining System: Implications for User Anonymity

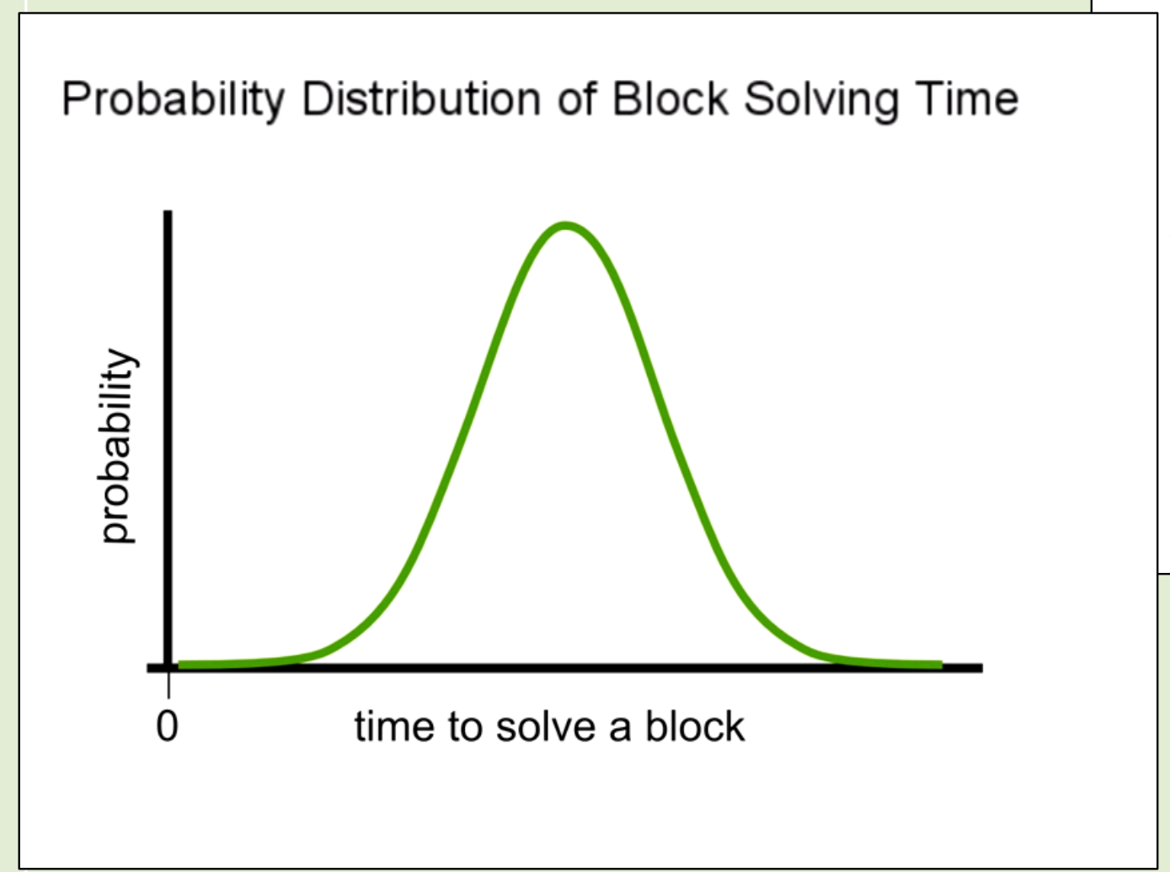
The Bitcoin cryptocurrency records its transactions in a public log called the blockchain. Its security rests critically on the distributed protocol that maintains the blockchain, run by participants called miners. Conventional wisdom asserts that the protocol is incentive-compatible and secure against colluding minority groups, i.e., it incentivizes miners to follow the protocol as prescribed. Below, I provide a breakdown of the blockchain's architecture and explain the structural flaws that result in an imperfectly secure Bitcoin platform. Through these, attacks on user anonymity by miners can occur and result in fraud.



Each block has a reference to the previous block. Transactions in the same block are considered to have occurred at the same time.

Because multiple people may be create blocks at the same time, there can be several options to choose from when determining what goes next in the chain. To mitigate this, each valid block must contain the answer to a complex mathematical problem. Miners are individuals who attempt random guesses to these problems, in the form of cryptographic hashes. The first person to solve a problem correctly has their block added next.





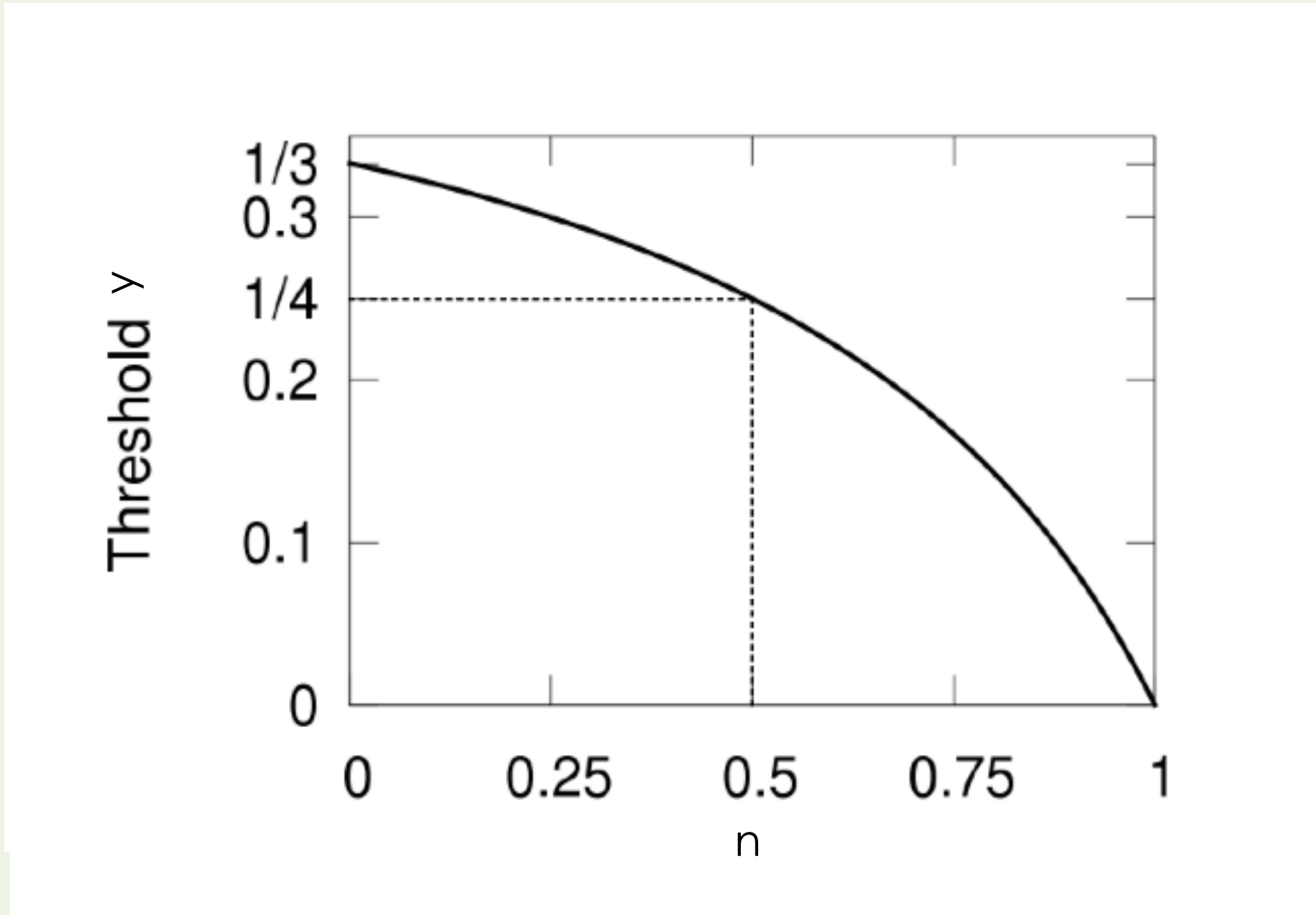
The randomness in a math problem effectively spreads out when it is that one finds a solution. While lucky guesses are possible, on average it takes everyone on the network the same amount of time to solve a block. In this way, the block chain is self-stabilizing, meaning that everyone is in agreement about the order of blocks at the end of the chain.

Mitigation of Colluding Miners

Commonly, miners "pool" together to solve blocks. The fact that these pools can be quite large has important implications for security. It is very unlikely for one attacking miner to solve many blocks in a row correctly, but this probability increases as a group of attackers' processing power increases in proportion to the rest of the network.

A possible solution exists against selfish mining pools that command less than ¼ of the Bitcoin resources. This threshold is better than the current reality where a group of any size can compromise the system. When a miner learns of competing branches of equal length in the blockchain, the miner should propagate all of them, and choose which one to mine uniformly at random. In the case of two branches, for example, this would result in half of the blocks being mined in the mining pool's branch and the other half mined in another branch.

Illustration of Mitigation Strategy



For a given n, the threshold shows the minimum power selfish mining pool that will trump the honest miner protocol. The current Bitcoin protocol allows n = 1, where a selfish mining strategy is always superior. Unrealistically favorable assumptions leave the threshold at 1/3. In contrast, the new, proposed protocol change achieves a threshold of ¼ by setting n = ½.

Conclusion

Bitcoin is the first widely popular cryptocurrency with a broad user base and a rich ecosystem, all hinging on the incentives in place to maintain the critical Bitcoin blockchain. This project analysis showed that Bitcoin's mining algorithm is not incentive-compatible. The Bitcoin ecosystem is open to manipulation and potential takeover by miners seeking to maximize their rewards. The threshold at which selfish mining is effective in the current Bitcoin system is close to zero, and by presenting a backwards-compatible modification to Bitcoin, it is possible to raise this threshold to ¼.

In the future, miner incentives and implementations of mitigation are unclear. Every four years, the block rewards that currently incentivize miners is cut in half - eventually, they will disappear altogether. It is likely, therefore, that sending money in Bitcoin will eventually no longer be a free process, and resultant shifts in economic incentives behind the use of Bitcoin will shift the system's privacy mitigation efforts.

References

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to Better — How to Make Bitcoin a Better Currency. *Financial Crytpography and Data Security*, *7397*, 399-414. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-32946-3_29#page-1

Eyal, I., & Sirer, E. G. (2013). Majority is not Enough: Bitcoin Mining is Vulnerable. *arXiv.org*. Retrieved from http://arxiv.org/pdf/1311.0243v2.pdf

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoyy, D., Voelker, G. M., & Savage, S. (2013). A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. *IMC '13 Proceedings of the 2013 conference on Internet*, 127-140. Retrieved from http://dl.acm.org/citation.cfm?id=2504747

Nakamoto, S. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from Bitcoin website: https://bitcoin.org/bitcoin.pdf