Ning Shi *Financial Innovation* (2016) 2:31
DOI 10.1186/s40854-016-0045-6

Financial Innovation

RESEARCH Open Access

A new proof-of-work mechanism for bitcoin

Ning Shi

Correspondence:
shiningchina08@126.com
School of Business, Sun Yat-sen University, Guangzhou, China

Abstract

Background: Bitcoin system, when more than 51% computing power is controlled by a single node, the block chain can be distorted maliciously. This is called 51% attack which is a well-known potential risk that could destroy the Bitcoin system.

Method: The paper proves that under the current proof-of-work mechanism, computing power eventually will be centralized at a single node if miners are rational enough.

Result: The paper propose a new proof-of-work mechanism that improves decentralization and reduces the risk of 51% attack without increasing the risk of Sybil attack.

Concusions: This new mechanism introduces a series of principles such as Career open to all talents, without distinction of birth, Distribution according to labor and All Men are created equal.

Keywords: Digital currency, Consensus mechanism, Bitcoin, proof-of-work

Background

Bitcoin, a peer-to-peer electronic currency, is a distributed ledger system (Nakamoto 2009). Every transaction is broadcast and verified by all nodes in the network through a particular consensus mechanism (Bonneau et al. 2015; Yermack 2013). Every node collects transactions in a block and the block is associated with a difficult mathematical problem. Solving that problem is called *mining*, and nodes that mine coins are called *miners*. The miner that solves the problem first secures the right to append the block to the current longest block chain. Once confirmed, the new block chain is then copied to every node in the network (Narayanan et al. 2016). The longest block chain is the *consensus* of all nodes, which records all transactions in the history.

Decentralization is the presiding feature of distributed ledger systems like Bitcoin. This feature, which contracts with other modern systems, are overseen by intermediaries. For example, the Society for Worldwide Interbank Financial Telecommunications (SWIFT) is central to the global payment system, such as, commercial banks for credit markets and central banks for monetary markets. All these centers prominent in other systems exert what is reasonably called political power, but Bitcoin functions without them. Bitcoin's supporters embrace the network's decentralization and have been proposing more aggressive formats such as a decentralized autonomous organization (Bannon 2016). A decentralized ledger can be maintained by a proof-of-work (POW) consensus mechanism

and reward incentive engineering. POW requires that nodes engage in mining to report verified blocks. This mining process consumes energy, time, and capital, but it prohibits malicious and penalty-free reporting.

The POW mechanism is essential to network security. Satoshi uses a *binomial random walk* model to prove that attackers must control 51% of the computing power in the system before they can generate the longest block chain by constructing fraudulent transaction records. This possibility known in the Bitcoin community as 51% attack is a major concern of Bitcoin system security. Although it seems unlikely that a single node could control more than half of the system's computing power, the computing power is actually controlled by a few major mining nodes (Fig. 1). We call this phenomenon computing power centralization. Some researchers also observe such phenomenon (Beikverdi and Song 2015). In this study, we aim to show how it can appear in a decentralized system. Moreover, will centralization eventually destroy the Bitcoin's decentralized system? (Gervais et al. 2014). We show that the computing power can be concentrated in a single node under the current POW design. When computing power is centralized, political power becomes decentralized. Therefore, we propose a new POW mechanism that encourages more nodes to participate in mining and reduces risk of a 51% attack.

Bitcoin mining

Mining Bitcoins requires significant computational resources. The Bitcoin network overall finds a block every 10mins, and locating a block in late 2014 necessitated computing 10^{21} SHA-256 hashes. Clearly, miners must invest in suitable computer hardware. First generation machines were CPUs in PCs , but it was impossible for CPUs to mine Bitcoins speedily as the difficulty of mining intensified. The second generation machines was GPUs on display cards, but miners found that only specialized and sophisticated machines, like ASIC, could earn profits. Successful miners update equipment quickly, and those who do not invest continuously and extensively in current-generation hardware must exit the industry or face the likelihood of never mining a single block out within

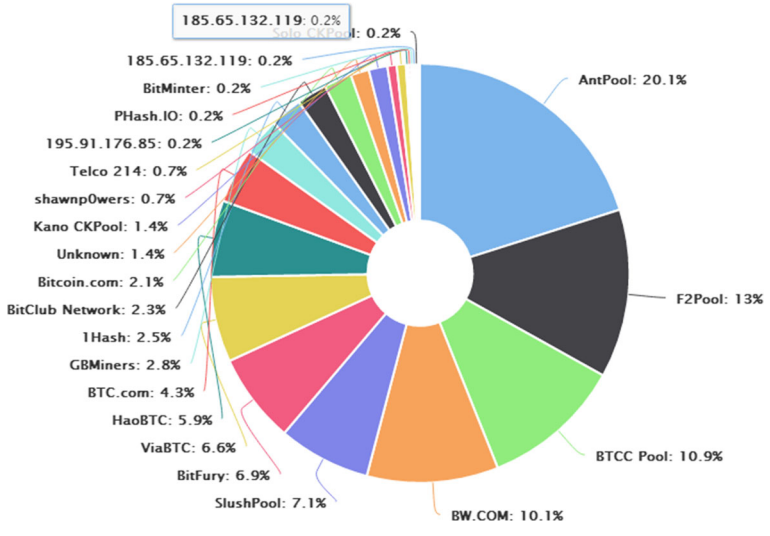

Fig. 1 Bitcoin computing power distribution

their lifetimes. Facing conditions of perpetual escalation, miners join pools, wherein they aggregate computational resources and share the rewards. Currently, pooled mining constitutes 72% of the Bitcoin's computation network.

Security

There are three blatant types of attacks on Bitcoin's security: Sybil attacks, block withholding attacks, and 51% attacks.

A Sybil attack uses multiple IDs to achieve its purpose. That is, one person or entity controls what appear to be multiple miners (Eyal and Sirer 2013; Miers et al. 2013).

In a block withholding attack, a miner who finds a winning solution, withholds it from the pool. This undermines earnings of everyone in the pool, including itself. Luu et al. (2015) studied a power-splitting games and showed that such attacks impair the system.

A 51% attack is described above and discussed in Nakamoto (2009). Some observes argue that 51% attacks are not incentive-compatible because attackers act to their own detriment (Vasek et al. 2014). As explained in Kroll et al. (2013), however, that is not necessary the case. For example, attackers who beforehand took short positions in Bitcoin-related equities, profit from the resulting price erosion.

Methods

Suppose Miner i owns percentage p_i of the system's total computing power. In Satoshi's design, mining difficulty can be adjusted per the time to create the last 2016 blocks to assure new blocks can be created every 10 min. We assume this interval is fixed. A similar analysis appears in (Rosenfeld 2011) but it disregards the *Bankrupt Probability*.

We define the investment in mining hardware by Miner i as m_i. Mining consumes energy. We denote the energy cost for a single time interval as e_i. After mining n epochs, the total cost is $(m_i r_i + e_i)n$ where r_i is the interest rate for one interval. We assume a Bitcoin's price, noted as bp, is constant and one block's reward is N Bitcoins.

Profit and loss analysis

We are interested in miner i's reward process. We can define an event of miner i successfully making block k valid as:

$$I_{ik} = \begin{cases} 1, & p_i, \\ 0, & 1 - p_i. \end{cases}$$

We take the process $\{I_{ik}, k = 1, 2, 3, ..., n, ...\}$ as an identical independent distribution (i.i.d). Then the total reward miner i can receive in n epochs can be written as

$$R_i = \sum_{k=0}^{n} I_{ik} * N * bp - (e_i + m_i r_i) * n.$$

R_i follows a binomial distribution with the mean and variance indicated below:

$$\mu(R_i) = N * bp * n * p_i - (e_i + m_i r_i) * n. \tag{1}$$

And its variance is

$$\sigma^2(R_i) = n * N * bp * (p_i + p_0)(1 - p_i - p_0) = (n * N * bp) * (p_i - p_i^2).$$

The business is sustainable only if $\mu(R_i)$ exceeds 0. That is, a solo miner survives if its computing power ratio satisfies:

$$\frac{p_i}{e_i + m_i r_i} > \frac{1}{N * bp}. \tag{2}$$

The above condition can be regarded as a criterion for screening qualified miners.

The first lucky time analysis

Lead times for acquiring the first coin are important for small miners. If it takes too long to complete the first block, the miner loses money and confidence. Even the miner who satisfies (2), it may not be sufficiently patient or wealthy to await the arrival of fortune's coming. Suppose the maximum tolerable loss for miner i is C_i which can be interpreted as a kind of budget.

We define the maximum tolerable time B_i

$$B_i = \frac{C_i}{e_i + m_i r_i}. \tag{3}$$

If Miner i cannot obtain a single block posted before B_i, he quits the business. Therefore, we investigate the time between any two consecutive events. As $\{I_i\}$ is indeed a Bernoulli process, the interval can be described by the following exponential distribution X_i with the rate parameter $= 1/p_i$.

$$P(X_i > B_i) = e^{-p_i B_i}.$$

This can be interpreted as the probability of bankruptcy for miner i. By introducing (2), we have,

$$P(X_i > B_i) = e^{-\frac{p_i C_i}{e_i + m_i r_i}}.$$

This probability increases with m_i and e_i and decreases with p_i, meaning that higher mining chances reduce the risk of bankruptcy.

We assume Miner i is risk-neutral and accepts business only when his probability of bankruptcy is less than β. Then, we have,

$$e^{-\frac{p_i C_i}{e_i + m_i r_i}} < \beta.$$

It is followed that,

$$\frac{p_i}{e_i + m_i r_i} > \frac{-\ln \beta}{C_i.} \tag{4}$$

Equations 2 and 4 present this circumstance for small miners as follows:

$$\frac{p_i}{e_i + m_i r_i} > \max\left\{\frac{-\ln \beta}{C_i}, \frac{1}{N * bp}\right\}$$

From the above analysis, the term $p_i/(e_i + m_i r_i)$ can be used to interpret the competitiveness of a miner. A miner with a larger $p_i/(e_i + m_i r_i)$ has less ruin risk.

Big pools dominate Bitcoin mining. Pools encourage individual miners to join, and accumulate computing power and profits for every node in the pool when a coin has been generated.

Suppose the pool Miner 0 has proportion p_0 of the system's computing power. By definition, $p_0 > p_i$. Miner i joins Miner 0, forming the enlarged pool Miner j. We first prove that miner j has a lower probability of bankruptcy than node i.

Proposition 1 *A smaller miner always reduces its probability of bankruptcy by joining a larger miner.*

Proof For the newly formed mining pool j, define I_{jk}:

$$I_{ik} = I_{i0} = I_{jk} = \begin{cases} 1, & p_i + p_0, \\ 0, & 1 - p_i - p_0. \end{cases}$$

The chance that Miner i will verify a block increases to $p_i + p_0$, but it receives only part of the reward each time it does so. We can rewrite

$$R_i = \frac{p_i}{p_i + p_0} \sum_{k=0}^{n} I_{ik} * Nbp - (e_i + m_i r_i) * n.$$

We then can show that,

$$\mu(R_i) = N * bp * n * p_i - (e_i + m_i r_i) * n.$$

Its variance is

$$\sigma^2(R_i) = \left(\frac{p_i}{p_i + p_0}\right)^2 n*bp*N*(p_i+p_0)(1-p_i-p_0) = \frac{p_i}{p_i + p_0} n*bp*N*\left(p_i - p_i^2\right).$$

This variance is much smaller than the original variance. Therefore, small miners can reduce its risk as the variance is reduced. □

Proposition 2 *The bigger miner is better off if a smaller miner joins it.*

Proof Similarly, we have

$$\mu(R_0) = np_0,$$

and, its variance is

$$\sigma^2(R_0) = \left(\frac{p_0}{p_i + p_0}\right)^2 n(p_i + p_0)(1 - p_i - p_0) = \frac{p_0}{p_i + p_0} n * bp * N * \left(p_i - p_i^2\right).$$

□

Although the reduction in variance is not as substantial as Miner i. Miner 0 is better off.

If pooling benefits both parties, why would they not pool? The answer explains the centralization of computing power and shows that even big miners have motivation to collaborate.

Proposition 3 *Pooling all miners produces the lowest variance.*

Proof Proposition 3 follows from Propositions 1 and 2. □

Results

If pooling works, we can make pooling as part of a new consensus mechanism described as below. The essential of the new mechanism is trying to separate the *Reporting Right* and the *Rewarding Value*, and it treats the whole system as a single pool. It turns out a set of *Socialism-style* principles are introduced in the new mechanism including *Distribution according to labor*, *A career open to all talents, without distinction of birth*, *All Men are created equal* and *The People's Congress Mechanism*. Improvements on Bitcoin are not

new, interested readers can find alternatives in (Andrychowicz et al. 2014; Heilman 2015; Karame et al. 2012; Kokoris-Kogias et al. 2016; Poelstra 2014).

A Socialism Bitcoin

Step 1. Design a mathematical problem that has $\mathbb{N}$ solutions rather than a single solution. Miner i may not find all solutions but a proportion of all solutions, for example, $\alpha_i * \mathbb{N}$ solutions.

Step 2. Once a miner finds out $\mathbb{N}$ solutions, he broadcasts his finding. Once miner i receives this message, he completes his work and reports the value α_i. When all α_j, $j \in S$ where S is the set of all nodes, are gathered, allocate miner i a proportion of $\frac{\alpha_i}{\left(\sum_{j \in S} \alpha_j\right)}$ rewards.

Step 3. Randomly generate a number b from $(c, 1)$, c must be greater than a cutoff value, for example 0.1 and choose the miner whose α_i is closest to b and let him submit the block. That is, it is not the miner who finish first submit the block. We introduce this randomness to further reduce the 51% attack risk.

Explanation: As Bitcoin is presently designed, miners must find a 32-bit nonce that causes its hash to be under a given target. Miners that find a valid nonce can submit their block. We label this aspect of Bitcoin's design as *Winners get all*. Miners with greater computing power have more chances to contribute to the formation of the longest consensus chain, creating the alternate phenomenon: *richer becomes richer*.

If a problem has multiple solutions, it may be possible to record how much efforts Miner i makes to identify a solution at a specific time. This finding would facilitate choosing miners from a number of miners rather than a single miner. We label this principle *Career open to all talents, without distinction of birth*.

By introducing the concept of partial solutions, every miner's work can be measured and appreciated. Measuring the workload requires the engineering introduced in Section Implementation details. We call this principle *Distribution according to labor*.

The new source of randomness that we introduce in this new protocol grants every node equal right to be selected to report the block. Doing so renders a 51% attack impossible because the chance to report the block is independent of computing power. It will not discourage miners from contributing as those with large computing power earn large rewards as they contribute more. We treat *reporting right* as a form of *political power* and the *computing power* as a form of *economical power*. Our new protocol eliminates the inevitability that miners with greater economical powers acquire greater political power, a principle we call *All Men are created equal*.

However, granting every node the right to report a block may engender Sybil attacks. A Sybil may duplicate numerous malicious nodes that entail little cost but augment chances to receive reporting rights. To reduce the risk of Sybil attacks, we introduce parameter c, which significantly increases the cost of an attack. In other words, not every participant has reporting rights, only those that finished more than $c * \mathbb{N}$ solutions. We call this *The People's Congress Mechanism*.

Introducing these principles achieves multiple benefits:

1. Every miner's risk of bankruptcy is reduced without sacrificing access to rewards, thereby increasing the system's stability.
2. It reduces the risk of 51% attack.

3. It is also not vulnerable to Sybil attack.
4. It also reduces the risk of Block withholding attack as reporting is not a solo.

Implementation details

Implementing our protocol requires solving at least two engineering issues:

1. **New puzzle design.** It can be done by decreasing the difficulty of the original Bitcoin's nonce searching problem and set the value of N according to some rule in order to guarantee a constant Bitcoin output rate.
2. α **counter.** It is an essential engineering problem to count α_i in every miner. The counter should be smart enough to remove duplicated solutions and store all correct ones. This issue is related to the first one. The design of the problem may lead to different counting methods.

Conclusion

Economists (Böhme et al. 2015) recognize that *Bitcoin has the potential to be a fertile area for social science research. Scholars should appreciate Bitcoin's contained environment with a clear set of rules (albeit not free from frictions), the publicly available record of transactions (unusual for most means of exchange), and the general availability of data even beyond the block chain (including market prices and trading volumes)*. The notion of Bitcoin as a social science laboratory is particularly attractive. We have proposed a protocol that introduces some socialism principles to reduce the risk of a 51% attack while encouraging miners' continued participation in the network. This study is far from mature and as noted issues of implementation need to be detailed. It nonetheless warrants future research from social scientists.

Authors' contributions

We prove that under the current proof-of-work mechanism, Bitcoin's computing power eventually will be centralized at a single node. We propose a new proof-of-work mechanism that improves decentralization and reduces the risk of malicious attack. All authors read and approved the final manuscript.

Competing interests

The authors have declared that no competing interests.

Received: 14 November 2016 Accepted: 30 November 2016
Published online: 22 December 2016

References

Andrychowicz M, Dziembowski S, Malinowski D, et al (2014) Secure multiparty computations on bitcoin. In: IEEE Symposium on Security & Privacy IEEE Computer Society. pp 443–458

Bannon S (2016) The Tao of The DAO. https://techcrunch.com/2016/05/16/the-tao-of-the-dao-or-how-the-autonomous-corporation-is-already-here/. Accessed 16 May 2016

Beikverdi A, Song JS (2015) Trend of centralization in Bitcoin's distributed network. In: 2015 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD) Vol. 00. pp 1–6. doi:10.1109/SNPD.2015.7176229

Böhme R, Christin N, Edelman B, Moore T (2015) Bitcoin: Economics, Technology, and Governance. The J Eco Perspect 29:213–238. doi:10.1257/jep.29.2.213

Bonneau J, Miller A, Clark J, et al (2015) Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. Security and Privacy IEEE, pp 104–121

Eyal I, Sirer EG (2013) Majority is not enough: Bitcoin mining is vulnerable. Computer Science 8437:436–454

Gervais A, Karame G, Capkun S, et al. (2014) Is Bitcoin a decentralized currency? IEEE Secur Priv 12(3):54–60

Heilman E (2015) One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner (Poster Abstract). Financial Cryptography and Data Security. Springer, Berlin Heidelberg. pp 161–162

Karame G, Androulaki E, Capkun S (2012) Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. IACR Cryptology ePrint Archive 2012:248

Kroll JA, Davey IC, Felten EW (2013) Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. The Twelfth Workshop on the Economics of Information Security (WEIS 2013) Weis, pp 1–21. Print

Kokoris-Kogias E, Jovanovic P, Gailly N, et al. (2016) Enhancing bitcoin security and performance with strong consistency via collective signing. pp 3–6. print arXiv: 1602.06997
Luu L, Saha R, Parameshwaran I, et al (2015) On power splitting games in distributed computation: The case of bitcoin pooled mining. In: 2015 IEEE 28th Computer Security Foundations Symposium. IEEE. pp 397–411
Miers I, Garman C, Green M, et al. (2013) Zerocoin: Anonymous distributed e-cash from bitcoin. In: 2012 IEEE Symposium on Security and Privacy Vol. 00. pp 397–411. doi:10.1109/SP.2013.34
Nakamoto S (2009) Bitcoin: a peer-to-peer electronic cash system. pp 1–9. Consulted
Narayanan A, Bonneau J, Felten E, et al (2016) Bitcoin and cryptocurrency technologies. Princeton University Press, New Jersey
Poelstra A (2014) Distributed consensus from proof of stake is impossible. https://download.wpsoftware.net/bitcoin/pos.pdf
Rosenfeld M (2011) Analysis of Bitcoin pooled mining reward systems. Computer Science December. arXiv preprint arXiv: 1112.4980 [cs.DC]
Vasek M, Thornton M, Moore T (2014) Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In: Böhme R, Brenner M, Moore T, Smith M (eds). Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science. Springer, Berlin Heidelberg Vol. 8438. pp 57–71
Yermack D (2013) Is Bitcoin a Real Currency? An Economic Appraisal. Handbook of Digital Currency. pp 31–43. Available at SSRN: https://ssrn.com/abstract=2361599