Does Miner Pooling Impact Bitcoin's Ability to Stay Decentralized?

David Sheehan
University College Cork
Cork, Ireland
112423328@umail.ucc.ie

Rob Gleasure
University College Cork
Cork, Ireland
R.Gleasure@ucc.ie

Joe Feller
University College Cork
Cork, Ireland
jfeller@ucc.ie

Phillip O'Reilly
University College Cork
Cork, Ireland
Phillip.oreilly@ucc.ie

Shanping Li
Zhejiang University
Hangzhou, China
shan@zju.edu.cn

Jerry Cristiforo
State Street
Jacristiforo@statestreet.com

OpenSym '17, August 23–25, 2017, Galway, Ireland

ACM ISBN 978-1-4503-5187-4/17/08.
https://doi.org/10.1145/3125433.3125462

Abstract

The Emerging Blockchain technologies have earned substantial attention in the area of Financial Technology in recent years. Its decentralized environment allows for the mining of Bitcoins by miners either independently or in groups. The community of miners have faith in the integrity of each other to sustain the network, through mining pools remaining at a reasonable level of mining power. Blockchain's decentralized system is one of its main selling points and is a source of great attraction for users. However, when these mining pools start to grow and increase their mining power to dangerous levels it can result in a shift towards a centralized environment. This push goes against foundational principles of Bitcoin, leading to ongoing debate among various stakeholders.

Author Keywords

Bitcoin; Blockchain; mining; mining pools; decentralization.

ACM Classification Keywords

Design, Security.

Mining: Mining is a process for ensuring the blockchain remains consistent and complete, whereby independent miners repeatedly collect and validate new broadcast transactions to create new 'blocks', which are only accepted by the rest of the network when they include some 'proof of work' linking it to the previous block (hence the name 'blockchain') [4]. Once validation is complete the nodes are forwarded to their neighbors. The network confirms the transaction by including it in the blockchain [3]. Bitcoin incentivizes mining by providing miners with new bitcoins in exchange for newly validated blocks. One strategy for miners seeking to increase rewards is to form mining pools which can achieve larger rewards. They also present a problem where mining pools can become large enough to destabilize a network if they adopt malicious practices to abuse decentralized validation processes [7, 10].

Introduction

Bitcoin is a peer to peer version of electronic cash that allows online payments to be sent from one party to another without the use of a 3rd party financial institution [11]. Its level of market capitalization has rapidly increased since it was launched in October 2008, and in the period from November 2014 to November 2016 it has more than doubled with a current level of over 19.92 billion US Dollars [2]. Bitcoin implements its decentralized system with a data structure called the 'blockchain', a distributed ledger that records copies of transactions on multiple nodes [6]. Blockchain technologies have been argued to possess a disruptive potential to rival the emergence of the Internet [9] and the decentralized structure of systems like Bitcoin create a number of benefits such as verifying and validating transactions, building trust and securing the network from malicious attacks [13].

This has led to significant discussion about Bitcoin and blockchain, including the security of a decentralized ledger, concerns over anonymity, transaction cost fees, and the speed at which transactions can be completed [12]. Fundamental to these concerns is the danger of relying on peer validation when the integrity of all actors can't be guaranteed [5, 8]. For example, the '51% attack', where a malicious user takes over the majority of the network and creates/validates false transactions [14]. This threat is not merely theoretical, as several other currencies have experienced similar attacks [15, 16, 17]. Bitcoin appears both unusually secure and unsecure in this regard. On one hand, the scale of the network makes such an attack seem far-fetched. On the other, 'mining pools' are becoming increasingly dominant in the peer validation process, to the point 3 pools are now responsible for over 40% of validation. This is creating an *ipso facto* centralization around these nodes, which are assumed to be trustworthy by those who continue to use the currency. To explain this tension, a Prisoner's Dilemma model of Bitcoin is proposed (see Figure 1).

		Miners	
		Mine in pools	Mine independently
Design-ers and Regulat-ers	Centralize	Adequately profitable for miners	Centralize
	Decentralize	Very profitable for miners	Decentralize

Figure 1. Prisoner's Dilemma view of Bitcoin

A thematic analysis method was adopted to expand this basic model. This analysis used (i) semi-structured interviews with 6 active Bitcoin miners and 6 Bitcoin designers/regulators (ii) participant observation of online discourse among miners and designers/ regulators for 4 months from February to May 2017.

Findings and Conclusions

Miners Believe Pooled Mining is Inevitable for Bitcoin

Existing research suggested mining pools were proving to be more profitable than independent mining. The costs of mining independently are high and it could take years to make a profit. The interviewees confirmed this, stating that independent pooling had been considered dead for a number of years and was not feasible in today's environment. Miner 3 commented, "Pooled mining is the only future we will see. Mining operations are likely to become more and more industrial in scale". Miner 1 explained "There is no point

Interview participants:

Admin 1	Blockchain consultant, Hyperledger advisor
Admin 2	North American Blockchain/Bitcoin expert
Admin 3	Bitcoin news Researcher
Admin 4	Irish Tech News Editor and FinTech expert
Admin 5	Bitcoin Expert South Africa
Admin 6	Blockchain/Bitcoin expert USA
Miner 1	Former Bitcoin Miner
Miner 2	Bitcoin Miner + Forum Moderator
Miner 3	Former Bitcoin Miner
Miner 4	Bitcoin/altcoin Miner + Forum moderator
Miner 5	Miner of altcoins
Miner 6	Bitcoin Miner

in solo mining nowadays, even back in 2013 I tried to mine Bitcoin and my hash rate didn't even register in the pool". The estimated number of tera hashes per second that the Bitcoin network is performing as of 19th April 2017 is 3,702,205 TH/s as opposed to 1000 TH/s in September 2013. It was around this time that the hash rate started to increase and since then it has soared to over 4,000,000 TH/s in January 2017 [1]. This hash rate level is proving impossible to compete with for solo miners in the Bitcoin environment. Hence, large pools such as Antpool, BitFury and F2Pool are continuing to take over from smaller pools and have wiped out the independent mining community. The market share that these large pools have is worrying and is leading to a centralization of the Bitcoin mining environment. Solo mining is more in line with the vision of a totally decentralized system of nodes. This shift to a centralized environment has led to independent miners moving away from the Bitcoin mining scene and trying their luck with some of the altcoins such as Dash (3.7 TH/s) and Monero (80.3 MH/s) as their hash rate is more manageable.

Designers/Regulators Have an Ideological Preference for Decentralization

Both miners and designers/regulators suggested they would prefer a completely decentralized environment. However, this preference appeared more ideological for designers/regulators, whereas many miners balanced this preference with the practical drive to make money from mining. Admin 4 lamented "Mining started out as a hobby for most people, however, it turned into money making. From this it has shifted from money making to circumventing capital controls and money laundering". Both sets of stakeholders saw global pooling as a diminishing decentralization. Admin 3 argued "Miners in China are attempting to hard fork the code into something more centralized". This creates a sense of tension concerning the intentions of some of these large groups among miners and designers/regulators.

Designers/Regulators are Struggling to Operationalize Alternatives to the Current Dominance of Mining Pools

Designers/regulators were concerned that the migration of almost all mining to a few dozen nodes in data centers around the world will make it easy for large malicious bodies to take over the currency. Admin 2 summed this up when they admitted, "The real potential threat to decentralization that we now face comes in a scenario where it becomes prohibitively expensive to run a full node at home. If all we have are a few dozen nodes set up in data centers around the world it would be very easy for state actors or criminals to influence these nodes and potentially change the network". Despite this threat, most interviewees felt that Bitcoin should not be regulated. The main reason for this opposition was the sense of futility associated with regulating such a rapidly evolving technology. Admin 4 noted "Bitcoin itself is basically impossible to regulate. Any attempts to do so only harm legitimate users and don't even slow down criminals".

Miners and Designers/Regulators Believe Equilibrium has Broken Down

Miners and designers/regulators were generally slow to predict what the network might look like in several years. Admin 1 stated that "I don't believe there is someone who can give a straight answer as regards an equilibrium in the future". Despite this uncertainty, most individuals felt confident in the future of the currency. The main reason for this was the sense that all of the parties with the power to harm the network

presently have a vested interest in its success. For example, no pool will want to act nefariously as it would cause a big decrease in hash power due to members leaving. Hence, the equilibrium between large pools such as Antpool, BitFury, F2Pool and a number of others can be seen in their level of hash rate distribution which are quite similar. This doesn't mean there isn't competition to increase the selfish share of mining among participants. Some miners are continuously trying to get the upper hand on competitors by using tools such as ASIC boost. Yet these selfish interests appear to be balanced as part of the larger user/consumer ecosystem.

REFERENCES

1. Hashrate Distribution. Blockchain.info, 2017. https://blockchain.info/pools?timespan=24hours.
2. CryptoCurrency Market Capitalizations. Coinmarketcap.com, 2016. https://coinmarketcap.com/.
3. Bamert, T., Decker, C., Elsen, L., Wattenhofer, R. and Welten, S. Have a Snack, Pay with Bitcoins. International Conference on Peer-to-Peer Computing, (2013), (pp. 1-5).
4. Barber, S., Boyen, X., Shi, E. and Uzun, E. Bitter to Better — How to Make Bitcoin a Better Currency. International Conference on Financial Cryptography and Data Security, (2012), (pp. 399-414).
5. Dion, D. I'll Gladly Trade You Two Bits On Tuesday For a Byte Today: Bitcoin, Regulating Fraud In The Economy of Hacker-Cash. University of Illinois Journal of Technology and Policy, (2013), (pp. 165-201).
6. Eyal, I. The Miner's Dilemma. IEEE Symposium on Security and Privacy, (2015), (pp. 89-103).
7. Eyal, I. and Gun Sirer, E. Bitcoin is Broken. Hacking Distributed, (2013).
8. Fabian, B., Ermakova, T. and Sander, U. Anonymity in Bitcoin – The Users' Perspective. International Conference on Information Systems, (2016).
9. Goel, S. Blockchain: The next big thing in technology?. The Economic Times, 2016.
10. Johnson, B., Laszka, A., Grossklags, J., Vasek, M. and Moore, T. Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools. International Conference on Financial Cryptography and Data Security, (2014), (pp. 72-86).
11. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. (2008).
12. Peters, G. and Panayi, E. Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. (2015).
13. Walsh, C., O'Reilly, P., Gleasure, R., Feller, J., Li, S. and Cristiforo, J. New kid on the block: A strategic archetypes approach to understanding the Blockchain. International Conference on Information Systems, (2016).
14. deMeijer, C. The UK and Blockchain technology: A balanced approach. Journal of Payments and Strategy, (2015), (pp. 220-229).
15. Litecoin Miners Urged to Leave Coinotron Pool Over 51% Threat. CoinDesk, 2014. http://www.coindesk.com/litecoin-miners-urged-leave-coinotron-51-threat/.
16. Krypton Recovers from a New Type of 51% Network Attack - Crypto Hustle. Crypto Hustle, 2016. https://cryptohustle.com/krypton-recovers-from-a-new-type-of-51-network-attack.
17. Dowd, K. and Hutchinson, M. Bitcoin Will Bite the Dust. Cato Journal, (2015), (pp. 357-382).