The Foggy Reality of Decentralization in Blockchain

In 2008, the irresponsible, fraudulent practices of large financial institutions led to the worst financial crisis since the Great Depression and exposed the pitfalls of a centralized financial system. In 2009, the pseudonymous Satoshi Nakomoto published the whitepaper for a peer-to-peer electronic cash system more widely known as Bitcoin. In other words, the first alternative for a more decentralized system came in the form of Bitcoin and its underlying blockchain technology. Since its inception, Bitcoin has grown to be valued at a market cap of over $500 billion and has paved the way for other blockchains with applications spanning beyond the realm of finance. Nevertheless, the rise of any technology over the past few decades has shown us not only its transformational nature, but also its inevitable shortcomings. When it comes to *existing* blockchain technologies, protocols and their applications, they all fall short of delivering *true* decentralization.

To understand why complete decentralization is impossible, it is imperative to first understand how current blockchains are designed and implemented. In essence, a blockchain is an immutable, distributed ledger of transactions consisting of nodes that work together to ensure the validity of all transactions. To achieve this, major public blockchains such as Bitcoin consist of a network of miners that append blocks of authenticated transactions to the chain. Miners are also required to solve difficult crypto-puzzles, known as Proof of Work, to ensure that one block is built about every ten minutes globally (Nakamoto, 2008). Solving these puzzles requires immense computing power only possible with application-specific integrated circuit (ASIC) computers used for the sole purpose of mining. As such, participation in these decentralized ecosystems is limited to individuals or companies with the necessary capital and computational power. An ordinary person is left using a currency that is hard to trace – sounds a lot like cash.

The distribution of mining power is highly skewed in the real world; governance decisions which have significant impact on the blockchain's development follow suit. In fact, a recent study at Cornell University found that 90% of the mining power is controlled by 16 miners in Bitcoin and 11 miners of Ethereum (Gencer et al., 2018). This means the blockchain is maintained by very few distinct entities. Since miners maintain the day to day on-chain activity, they effectively have a large influence on updates to the platform's software that they use. However, these updates are not only minor bug fixes, but also monumental proposals such as deciding on whether to establish a finite monetary supply for Bitcoin – which was voted on and approved in 2018. Similar to mining, such governance and decision making is concentrated within a "core" development community (Chu & Wang, 2018). Cryptocurrencies aimed to replace the trust placed in centralized institutions by fiat currency with trust in a peer-to-peer network that anyone, theoretically, could participate in. This theoretical shadow of decentralization covers a reality of recentralization from central banks to a small group of miners and developers.

Decentralized Finance, "DeFi," emerged over the past few years as a revolutionary application of blockchain, using automated on-chain protocols to provide financial services without intermediaries. However, as is the case for blockchains and the applications they support, both merely purport to be decentralized. All DeFi platforms have central governance frameworks outlining how to set strategic and operational priorities. Thus, all DeFi platforms have an element of centralisation, which typically revolves around holders of "governance tokens" (often platform developers) who vote on proposals similar to corporate shareholders (Aramonte et al., 2021). Furthermore, some DeFi blockchains are inherently designed to favor the concentration of decision power in the hands of large coin-holders. While some major

blockchains like Bitcoin incentivize participation through Proof of Work, other blockchains such as Ethereum achieve this through Proof of Stake (PoS), which is expected to also improve scalability. Staking is similar to putting money in a high-yield savings account; PoS encourages validators to stake more of their coins so that they have a higher chance of "winning" the next block and receiving compensation. Since the associated operational costs are mostly fixed, this setup naturally leads to a concentrated, small group of participants (Auer et al., 2021). The reasons behind the illusion of decentralization in DeFi point to a larger issue that puzzles experts to this day.

An obvious alternative to the concentration of mining and governance is increasing the number of participants to include everyone who wishes to do so. However, in addition to the barriers in acquiring the necessary resources, there is a scalability issue that arises with the increasing number of nodes and transactions in blockchain. Since every node needs to store and validate every transaction, increasing the number of participants has detrimental effects on the speed of transactions and the broader blockchain network. This tradeoff between decentralization and scalability – along with the essential propriety of security – was coined the “scalability trilemma,” by Vitalik Buterin, the co-founder of Ethereum (Khan et al. 2021). Ultimately, the scalability trilemma states that trade-offs are inevitable among these characteristics of blockchain. Despite Buterin discussing this issue, the description of the Ethereum blockchain explicitly mentions “a global, decentralized platform for money and new kinds of applications.” This is the epitome of decentralization in all major blockchains; while most tout themselves as decentralized, there are other factors and tradeoffs hindering its manifestation in the real world.

After understanding the current nature of blockchain technology and how it is designed and implemented in practice, the major challenges for blockchain decentralization are evident:

skewed mining power and decision making as well as the inherent conflict between decentralization and scalability. The technology does provide an alternative to large centralized institutions, but achieves this through concentrating trust and decision making in the hands of a slightly more benevolent community of participants such as miners and developers. As long as scalability issues continue to plague blockchain, achieving the current ideal of decentralization will remain nearly impossible. However, all hope is not lost for working towards a more decentralized system as flaws in technology pose the opportunity for new technology that solves them.

Works Cited

Aramonte, S., Huang, W. and Schimpf, A., 2021. *DeFi risks and the decentralisation illusion*. BIS Quarterly Review. [online] Bank for International Settlements. Available at: <https://www.bis.org/publ/qtrpdf/r_qt2112b.htm> [Accessed 23 May 2022].

Chu, S. and Wang, S., 2018. *The Curses of Blockchain Decentralization*. [ebook] University of Washington and Epichain.io. Available at: <https://arxiv.org/pdf/1810.02937.pdf> [Accessed 23 May 2022].

Gencer, A., Basu, S., Eyal, I., van Renesse, R. and Gun Sirer, E., 2018. *Decentralization in Bitcoin and Ethereum Networks*. [ebook] Initiative for Cryptocurrencies and Contracts & Computer Science Department, Cornell University. Available at: <https://fc18.ifca.ai/preproceedings/75.pdf> [Accessed 23 May 2022].

Hoffman, M., Ibanez, L. and Simperl, E., 2020. *Toward a Formal Scholarly Understanding of Blockchain-Mediated Decentralization: A Systematic Review and a Framework*. Blockchain for Good. [online] frontiers in Blockchain. Available at: <https://www.frontiersin.org/articles/10.3389/fbloc.2020.00035/full#footnote3> [Accessed 23 May 2022].

Khan, D., Jung, L. and Hashmani, A., 2021. *Systematic Literature Review of Challenges in Blockchain Scalability*. [online] Multidisciplinary Digital Publishing Institute. Available at: <https://www.mdpi.com/2076-3417/11/20/9372> [Accessed 23 May 2022].

Nakamoto, S., 2009. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [ebook] Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 23 May 2022].