Is There a Future for Proof-of-Work Blockchains?

Task 1 - 41029 Engineering Research Preparation

Michael Larsen

Student ID: 12941783

Distributed ledger technologies, such as blockchain have become a buzzword in the technology world, given its potential across various industries. Early Proof-of-Work (PoW) blockchains used with Bitcoin and Ethereum consume large amounts of energy and process transactions slowly to achieve acceptable levels of security. Microsoft founder, Bill Gates is quoted saying "Bitcoin uses more electricity per transaction than any other method known to mankind" (ClubhouseConvo, 2021). Without the ability to support high transactional throughput, these technologies with slow transaction speeds, negative environmental and economic implications may not be competitive to current infrastructure. This essay will analyse PoW blockchains in terms of their environmental, social, and technical impacts and determine if there is a future for these technologies. Furthermore, this essay will draw upon existing literature, viable solutions, and alternative technologies.

A blockchain is a type of distributed ledger that collects data together in groups, known as blocks. These blocks hold sets of information and once they reach their storage capacity, they are chained onto the previously filled block, forming the blockchain. To validate and confirm the data, blockchain uses PoW, which is a mechanism that requires members of a network to expend effort to deter malicious uses of computer power (Frankenfield, 2021). To further understand how this is implemented, it is instructive to view it in the context of Bitcoin.

Bitcoin is a decentralised digital currency, that uses blockchain for peer-to-peer transactions. When a user wants to send another user Bitcoin, it is broadcasted into the Bitcoin network, picked up by a Bitcoin miner and added to their list of unconfirmed transactions. Bitcoin miners then take these transactions and store them into the next block to be mined. To be selected to create the next block, they use computational power to solve complex problems. Once solved, the block is added to the blockchain.

The Bitcoin miners receive Bitcoin as a reward for completing blocks of transactions. These rewards, however, are only paid to the miner who discovers a solution to the problem first. The probability that a miner will be the first to discover a solution is proportional to their computational power. The computational power required to solve these problems requires large amounts of energy. According to the University of Cambridge, they currently estimate that the global energy consumption of computers that mine Bitcoin, amounts to 94 terawatt-hours per year (CBECI 2021). Comparatively, Google used 12.7 terawatt-hours globally in 2019 (Jaganmohan 2021). With sustainable development and climate change becoming one of

the major challenges that society is facing, Bitcoin may not be a viable competitor to current peer-to-peer transactions.

There are three fundamental features that need to coexist for Bitcoin and other distributed ledger technologies to succeed. Firstly, scalability; it needs to demonstrate a capacity to handle a certain number of transactions without processing issues and delays. Secondly, decentralisation; equally distribute control over the network to all participants. Thirdly, security; prevent malicious entities from taking over. These three fundamental features form what is referred to as the 'Blockchain Trilemma', coined by Vitalik Buterin, co-founder of Ethereum.

The blockchain trilemma describes that the three fundamentals cannot coexist without the sacrifice of one. As an example, lets analyse the scalability of Bitcoin. Scalability is often calculated by the capability of a network to handle large amounts of transaction data in a short span of time. The Bitcoin network can process a maximum of 7 transactions per second and each transaction takes about 10 minutes to be confirmed (Decentralized Dog 2020). To put that into perspective, traditional payment providers such as VISA, have the capacity for 65,000 transactions per second (Visa 2017).

Bitcoin's shortfall is due to the blocks it uses to process transactions, as each block can only store a maximum of 1MB (Megabyte) of data. An obvious solution would be to increase the storage capacity of each block, resulting in more transactions per second. However, a larger block would require more computer power, resulting in fewer bitcoin miners possessing the required power, leading to more centralisation. Another solution is Bitcoin's Lightning Network, which is a second layer added to Bitcoin's network enabling transactions off the blockchain (Sharma 2021). The Lighting Network is designed to increase transaction speeds and decrease associated costs. However, security is an issue with research from the Hebrew University of Jerusalem (Bambrough 2021) showing that a relatively low resource actor could leverage an attack putting funds at risk.

Currently, the present infrastructure of Bitcoin fails to address all three fundamental features at once. Therefore, it doesn't appear to position itself as a reputable payment network and competitor to current infrastructure. This topic, however, has been widely studied to find reliable solutions. Zhou et al. (2020) present two possible solutions, blockchain pruning and

sharding techniques. Blockchain pruning consists of removing some historical data that isn't critical from the blockchain while preserving security. The reduction of data would release the storage pressure of blocks and allow for more efficiency. The sharding technique can be used to split the blockchain up into several smaller networks to balance the networks load across many networks. However, these solutions are still open for further investigations.

Yanagihara and Fujihara (2021) proposed a cross-referencing method for enabling multiple peer-to-peer network domains to manage their own public blockchains to improve scalability whilst maintaining decentralisation and security. They theoretically evaluated their method and concluded that it can reach the same level of transactions as current infrastructure, such as Visa. They also concluded that the method improved the tamper-resistance of blockchain while reducing the degradation of decentralisation.

Nonetheless, the topic of energy consumption remains. Sedlmeir et al. (2020) describes an alternative consensus mechanism; Proof-of-Stake (PoS), to replace the energy intensive PoW mechanism. PoS removes the computationally intensive steps involved with solving complex problems in PoW and instead relies on users to validate transactions and create new blocks based on their stake, alleviating the need for large computer power and energy consumption. They concluded that the computational complexity of PoS blockchains is low and not affected by network size and that the energy consumption is substantially lower than that of PoW blockchains.

Schueffel (2018) suggests that alternative technologies might be the solution to the blockchain trilemma, specifically hashgraph (p. 4-5). Hashgraph is a different method of sharing information to establish consensus by using the gossip protocol, where nodes pass on information in a way that if a single node becomes aware of new information, it will spread exponentially through the network until all nodes are aware of it. Hashgraph can handle more than 10,000 transactions per second and confirm transactions within seconds (Hedera Hashgraph 2021) and according to Olcott (2020), Hedera, which uses hashgraph, requires 5 million times less energy per transaction compared to Bitcoin.

There are however uncertainties and risks associated with the implementation of the aforementioned solutions. With the technology currently available, it appears that scalability can only be reached by sacrificing security or decentralisation. To feature scalability without

sacrifice, PoS could be implemented. Moving away from PoW can have ethical implications, as it moves away from the foundations that Bitcoin was built on. There are also risks with moving towards a more centralised solution as it can introduce imbalance and destroy individual initiative. With reduced security, malicious users can disrupt the network and access valuable data, making the blockchain network impractical. Security comes at the cost of energy consumption and scalability with the current Bitcoin PoW consensus mechanisms. These uncertainties and risks need to be addressed and further research into PoS, sharding, cross-referencing and hashgraph is required to present a viable solution and determine if there is a future for PoW blockchains.

Reference List

Bambrough, B. (2021, July 09). *Bitcoin's Lighting Network Is Struggling To Overcome Fundamental Issues.* https://www.forbes.com/sites/billybambrough/2020/07/09/bitcoins-lightning-network-is-struggling-to-overcome-fundamental-issues/

CBECI. (2021). *Bitcoin network power demand.* https://cbeci.org/

ClubhouseConvos. (2021, February 25). *Andrew Ross Sorkin Interviews Bill Gates in. Clubhouse* [Video]. Youtube. https://www.youtube.com/watch?v=VQFNb93q3CI

Decentralized Dog. (2020, September 30). How Long Does a Bitcoin Transaction Take? *Crypto Basics.* https://coinmarketcap.com/alexandria/article/how-long-does-a-bitcoin-transaction-take

Frankenfield, J. (2021, July 22). *Proof of Work (PoW).* https://www.investopedia.com/terms/p/proof-work.asp

Hedera Hashgraph. (2021). *The 3rd generation public ledger.* https://hedera.com/

Jaganmohan, M. (2021, March 24). *Google's energy consumption FY 2011-2019.* https://www.statista.com/statistics/788540/energy-consumption-of-google/

Olcott, J. (2020). *Can a Blockchain be Green?* Power Transition. ptvolts.com. https://ptvolts.com/sites/default/files/documents/sustainable-blockchain-power-transition.pdf

Schueffel, P. (2018). *Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph – A High-Level Overview and Comparison.* Institute of Finance, School of Management, Fribourg, Switzerland

Sedlmeir, J., Buhl, H., Fridgen, G., Keller, R. (2020). *The Energy Consumption of Blockchain Technology: Beyond Myth.* Business & Information Systems Engineering (62), 599-608.

Sharma, R. (2021, March, 2021). *Bitcoin's Lighting Network: 3 possible Problems.* https://www.investopedia.com/tech/bitcoin-lightning-network-problems/

Visa. (2017, August 09). *Visa Fact Sheet*. visa.com. https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf

Yanagihara, T., Fujihara, A. (2021). *Cross-Referencing Method for Scalable Public Blockchain.* Department of Information and Communication Systems Engineering, Chiba Institute of Technology, Japan

Zhou, Q., Huang, H., Zheng, Z., Bian, J. (2020). *Solutions to Scalability of Blockchain: A Survey.* IEEE