Defects analysis of blockchain PoW consensus protocol

Yungui Chen*, Liwei Tian, Lei Yang, Longqing Zhang, Yong Fan
School of Computer Science, Guangdong University of Science and Technology, Dongguan, Guangdong, China

ABSTRACT

Blockchain technology represented by cryptocurrencies has increasingly become the focus of social attention. The consensus protocol is the foundation for how the blockchain works. PoW, as the most widely used protocol, received more attention from researchers. This paper analyzes the defects of PoW, the most popular public chain consensus protocol in Blockchain, from five perspectives and points out the natural defects of PoW in high energy consumption, electronic waste, carbon footprint, expensive transaction fees, and centralization. This paper encourages the use of PoS and DPoS protocols instead of PoW protocols as they reduce the intensity of competition and may address the root cause of the aforementioned issues.

Keywords: PoW consensus protocol, blockchain, defects analysis

1. INTRODUCTION

Blockchain is a decentralized ledger with strong tamper resistance. Peer nodes distributed in different locations maintain the blockchain system's operation through cooperation, and the consensus protocol is the unified rule of cooperation between peer nodes. Blockchain systems can be divided into the public Blockchain, consortium blockchain, and private Blockchain according to different ways of node participation. Consortium[1] and private chains belong to non fully open Blockchain; the system sets a threshold for joining. For example, only nodes authorized by the Certificate Authority (CA) can join the maintenance of the Blockchain. The public chain is entirely open. Anyone can act as a node in the network without permission or authorization from anyone. The public chain is currently the most widely used blockchain system, and the PoW protocol is also the most widely used consensus protocol in the public chain[2] systems.

However, the essence of the PoW protocol is a useless competition for computing power[3]. The winner becomes a leader, obtains the right to package blocks, and obtains rewards and transaction fees. Driven by interests, mining industry participants continue to improve their computing power, making the protocol increasingly exposed to various defects. Nakamoto created the PoW mechanism to avoid human nature, so let machines participate in the workload competition. He pursues true decentralization and a fair way of wealth distribution. His point-to-point e-cash system attracted many liberal geeks to form a large community.

This paper's contribution is to analyze the PoW protocol's defects from five angles and point out that PoS and DPoS are alternatives to the PoW protocol.

2. POW PROTOCOL AND MINING

Induced by economic interests, peers compete for the right to package blocks, the process known as mining. The PoW protocol essentially uses a computer to solve a complex mathematical problem, and the first one to find a specific solution is rewarded. The PoW mechanism refers to the requirement to show specific proof to indicate the workload. For the work accumulated by small probability events, showing the result is equivalent to proving the workload. In the mining industry, the workload is equivalent to the computing power. The computing power of the node is strong, and the workload is naturally large at the same time. The competition for block packaging rights is a competition for computing power[4]

$$BlockHash = Hash(otherheader + Nonce) << D \quad (1)$$

* chenyungui@gdust.edu.cn

Third International Conference on Computer Science and Communication Technology (ICCSCT 2022)
edited by Yingfa Lu, Changbo Cheng, Proc. of SPIE Vol. 12506, 125061T
© 2022 SPIE · 0277-786X · doi: 10.1117/12.2662213

$$otherheader = previousBlockHash + merkleRoot + timeStamp \quad (2)$$

Equations (1) and (2) describe the mathematical logic of PoW mining. D is the target difficulty value, and merkleRoot is the root hash value for all transaction lists that must be packaged in blocks according to the Merkle tree. The mining process is to try different nonce to get BlockHash close to D.

Because the computing power involved in mining is changing (usually developing in a more significant direction), the block interval of 10 minutes is an important parameter to ensure the regular operation of Bitcoin. Therefore, for every 2016 blocks in the Bitcoin system, all nodes will automatically adjust the difficulty according to Equation (3). It increases the difficulty if the block generation rate is faster than 10 minutes and decreases the difficulty if it is slower than 10 minutes.

$$Difficulty_{new} = Difficulty_{old} * (t_{all} / 2016 * t_{avg}) \quad (3)$$

Where t_{avg} values of 10 minutes, t_{all} represents the time the system took to generate 2016 blocks in the past. By executing Equation (3), the system can maintain a block interval of about 10 minutes[5].

3. DEFECTS ANALYSIS

3.1 High energy consumption

With more and more equipment participating in mining and more substantial computing power, the energy consumption of Bitcoin and Ethereum is increasing every year, and the power consumption is also skyrocketing, resulting in massive energy consumption. Moreover, the mining solution process has no value other than proving who should be rewarded. Therefore, mining is considered a severe waste of resources. The electricity consumption of the Bitcoin network in 2019 has already exceeded the electricity consumption of the entire country of Belgium[6]. Figure 1 reveals the trend of bitcoin electricity consumption since 2012. The data comes from CBECI[7].

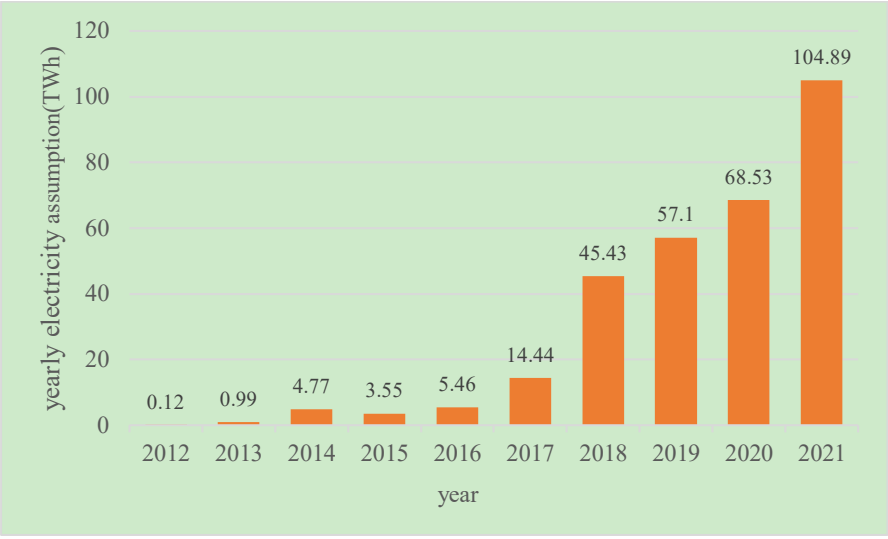

Figure 1. Bitcoin's annual electricity consumption from 2012 to 2021.

3.2 Electronic waste

In order to get more payouts, miners are constantly upgrading their mining equipment. Table 1 shows several stages of mining equipment. At first, people used ordinary computers and GPU graphics cards to mine but later upgraded to mining machines designed specifically for mining.

For CPU and graphics card mining machines, even if they are not used for mining, they can be used as ordinary computers. For FPGA mining machines and ASIC mining machines, if they are not used for mining, they can only be scrapped.

Table 1. Mining machine classification.

Mining machine type	Explanation
CPU mining machine	The earliest mining machine was a home computer. To mine through the CPU, ordinary people could become miners at home.
Graphics card mining machine	Graphics GPU chips are mainly produced by two suppliers, AMD and NVIDIA.
FPGA mining machine	It can be regarded as a transitional mining machine, using FPGA programmable chips as the core.
ASIC mining machine	The mining efficiency is extremely high, and it can perform trillions of hash operations per second, equivalent to the computing power of one million CPUs.

E-waste refers to abandoned mining machines. The life cycle of mining machines is generally two to three years. Although they can continue to work after two to three years, the possibility of mining "mines" becomes very small. With the system cranking up the mining difficulty factor, the electricity costs will not offset the mining output if miners continue to use older equipment. As a result, these mining devices designed explicitly for pow will be spontaneously phased out and become electronic waste. The e-waste generated by the cryptocurrency mining industry has become a significant issue. The literature[8] states that Bitcoin generates 30.7 kilotons of e-waste annually, equivalent to the amount of telecommunications equipment waste produced by countries such as the Netherlands.

3.3 Carbon footprint

In December 2018, the World Health Organization and the International Energy Agency jointly announced that after comparing the data of 135 countries, the 20 countries with the highest and lowest per capita carbon emissions were obtained. At the same time, it also announced that global warming caused by human-caused climate change is real. Research shows that backward countries' per capita carbon emissions are extremely low due to the lack of industrial facilities and even the inability to guarantee power supply. The higher the income of countries, the higher the per capita carbon emissions. For example, the highest per capita carbon emission in Qatar is about 600 times that of the Democratic Republic of Congo, reaching a terrible level of 35.73 tons of carbon dioxide per person per year.

Since mining requires much electricity, colossal greenhouse gas emissions follow when high-carbon power generation methods such as coal and petrochemicals are still the primary electricity source for human society. Worse, prominent blockchain miners are primarily distributed in underdeveloped areas, exacerbating the final carbon emissions. Research shows that Ethereum's carbon emissions are equivalent to Hong Kong's[7].

3.4 Expensive transaction fees

Equation (4) describes that a miner's mining revenue consists of rewards and transaction fees.

$$profit = reward + \sum_{i=1}^{n} transactionFee_i \tag{4}$$

The reward that can be obtained from Bitcoin mining is halved every four years, which is an exponential decrease. Therefore, if miners want to maintain the same income, they can only rely on the transaction fee attached to each transaction, which means the burden on the transaction initiator will increase. Ethereum, which also uses PoW as a consensus protocol, faces the same dilemma. We have observed that the minting and exchanging fees for Ethereum-based NFTs are generally tens to hundreds of dollars. The minting fee for "CloneX #10673" is $19.2, and the minting fee for "Hooligan #1951" is $31.11.

3.5 Centralization

Those who have the technology and are rich can obtain and develop more sophisticated mining equipment, which is equivalent to monopoly computing power, which runs counter to the decentralization of Blockchain. At the same time, because of selfish mining pools, blockchain centralization is becoming more serious. The Hash distribution shows that the largest 11 mining pools account for almost 100% of the Bitcoin network's computing power (the portion marked as unknown is the remaining share). In descending order, Bitcoin's share of computing power is Foundry USA, AntPool, F2Pool, Poolin, ViaBTC, Binance Pool, SlushPool, BTC.com, Luxor, SBI Crypto, unknown, and KuCoinPool.

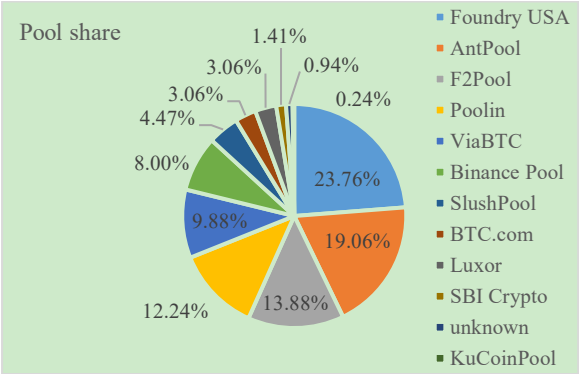

Figure 2. Bitcoin's computing power distribution

4. SOLUTIONS

From the above five perspectives, PoW is not an excellent consensus protocol. PoS[9] and DpoS[10] are alternatives to PoW consensus currently recognized by the academic community, and they both improve consensus performance from the perspective of reducing fierce competition among miners. In essence, reducing competition means reducing the investment of all miners, which makes it possible to reduce energy consumption.

4.1 Analysis of PoS advantages

PoS (Proof of Stake) is a system that distributes interest according to the amount and time of coins held by miners. In the PoS model, the miners' "mining" income is proportional to the coinage; that is, the miner with a higher coin age becomes the leader, while the miner with a higher coin age becomes the leader. The computing performance of the device is irrelevant.

Taking 140,000 mining participants as an example, if PoS is chosen instead of PoW, the energy consumption can be reduced by 99%. Due to the introduction of the "coin age" in PoS consensus, the mining difficulty is significantly reduced, so ordinary computers can be competent for mining, and one PC can run multiple mining clients simultaneously, significantly reducing energy consumption. The "retired" mining machine computer can be used for daily office use, thereby reducing the possibility of electronic waste generation, which is different from the "non-mining or scrapping" situation of the PoW mining machine. At the same time, the PoS consensus also retains the high openness of the public chain.

4.2 Analysis of DPoS advantages

DPoS (Delegated Proof of Stake) is a consensus algorithm based on voting. The token holder elects several representative nodes to operate the network, and professionally run network servers are used to ensure the security and performance of the blockchain network. In the DPoS mechanism, there is no need for computing power to solve mathematical problems, but the coin holder elects the producer. If the producer is incompetent, he may be voted out at any time, which also solves the performance problem of PoS[11].

In the experiment comparing PoW and DPoS, we determine that since DPoS adopts the rotating mining mechanism, the orphan block problem in the PoW consensus is effectively avoided. When DPoS consensus is executed on an ordinary personal desktop computer, the block generation speed can reach 3 seconds per block or even 1 second per block, significantly improving the system's throughput and reducing transaction latency.

In conclusion, both PoS and DPoS will be suitable alternatives to PoW consensus from multiple dimensions such as social responsibility, transaction fees, and performance metrics.

5. DISCUSSION

There has been disagreement over the replacement of PoW with PoS and DPoS. Opponents argue that PoS and DPoS undermine the decentralized nature of the Blockchain. Because PoS uses stake as a ruler, the rich are in power. The power in the DPoS is concentrated in the hands of the elected. We believe these concerns are unnecessary. As shown in Figure 2, the power centralization of PoW is also very serious over time, and this situation is not better than PoS and DPoS. It is reported that the implementation date of the merger and upgrade of Ethereum's consensus algorithm to PoS is September 19, 2022, which caused a shock to the entire cryptocurrency industry. Merging the PoS-running beacon chain with the PoW-running original chain and phasing out the PoW part of the original chain, this upgrade represents a switch to PoS consensus soon for Ethereum.

The application of DPoS in EoS as an example, the system can eventually achieve millions of transactions per second, with no transaction fees, security, and no forks. Correspondingly, decentralization is sacrificed to weak centralization or a multi-centralized model. After all, everything is a trade-off. DPoS abandons part of the decentralization in exchange for a geometric increase in performance and security.

6. CONCLUSION

PoW is currently the most widely used consensus protocol in public Blockchain, but the anti-PoW voices are also loud. This paper analyzes the natural flaws of PoW protocols in terms of high energy consumption, electronic waste, carbon footprint, expensive transaction fees, and centralization. This paper encourages using PoS and DPoS to replace PoW protocols and analyzes the advantages of PoS and DPoS over PoW. PoS and DPoS protocols reduce the intensity of competition and can address the root cause of the above problems.

ACKNOWLEDGMENTS

This work was supported by the Key Scientific Research Platforms and Projects of Colleges and Universities in Guangdong Province, Special Projects in Key Fields (natural science)(Grant No. 2021ZDZX1075), Natural Sciences Project of Guangdong University of Science and Technology(Grant Nos. GKY-2020KYYBK-24 and GKY-2020KYYBK-27), Innovative and Strengthening Project of Guangdong University of Science and Technology(Grant Nos. GKZLGC2021092, GKY-2019CQYJ-3, and CQ2020062), College Students Innovation Training Program held by Guangdong University of Science and Technology(Grant Nos. 1711034, 1711080, and NO.202013719006X).

REFERENCES

[1] Li, Z. et al., "Consortium blockchain for secure energy trading in industrial internet of things," IEEE Transactions on Industrial Informatics, 1-1, (2017).
[2] Houben, R. and Snyers, A., "Cryptocurrencies and blockchain," Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion, 1-86(2018).
[3] Li, A., Wei, X., and He, Z., "Robust proof of stake: A new consensus protocol for sustainable blockchain systems," Sustainability, 12(7), 2824(2020).
[4] Meneghetti, A., Sala, M. and Taufer, D., "A survey on pow-based consensus," Annals of Emerging Technologies in Computing (AETiC), (2020).
[5] Noda, S., Okumura, K. and Hashimoto, Y., "An economic analysis of difficulty adjustment algorithms in proof-of-work blockchain systems," SSRN, 3410460(2019).
[6] De Vries, A., "Bitcoin's energy consumption is underestimated: A market dynamics approach," Energy Research and Social Science, 70, 101721(2020).
[7] Gallersdörfer, U., Klaaßen, L. and Stoll, C., "Energy consumption of cryptocurrencies beyond bitcoin," Joule, 4(9), 1843-1846(2020).

[8] De Vries, A. and Stoll, C., "Bitcoin's growing e-waste problem," Resources, Conservation and Recycling, 175, 105901(2021).
[9] Saleh, F., "Blockchain without waste: Proof-of-stake," The Review of Financial Studies, 34(3), 1156-1190(2021).
[10] Chauhan, A., et al., "Blockchain and scalability," 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 122-128(2018).
[11] Zhang, S. and Lee, J.-H., "Analysis of the main consensus protocols of blockchain," ICT Express, 6(2), 93-97(2020).