The Performance Comparison between PoSpace and PoW

Zheng Wang*

School of Artificial Intelligence and Data Science, Hebei University of Technology, Tianjin, China

*Corresponding author: 205238@stu.hebut.edu.cn

Abstract. The consensus algorithm of Bitcoin, namely proof-of-work (PoW), has been criticized for its high energy consumption and centralization of mining power. PoW needs a lot of processing power to execute cryptographic problems and verify network transactions. In contrast, Chia's consensus mechanism is based on proofs-of-space (PoSpace), which utilizes disk space rather than computing power. PoSpace involves generating a large amount of verifiable storage space on the network and requires less energy consumption than PoW. This paper presents a comparative analysis of the algorithms used by Bitcoin, Ethereum, and Chia. The paper simulates the PoW and PoSpace processes by Java and compares both mechanisms' memory, CPU usage, and time consumption using VisualVM. The experiment results show that PoSpace costs less space and time resources than PoW. The former is more energy-efficient and decentralized.

Keywords: Cryptocurrency; Consensus Algorithms; Chia; Bitcoin; Proofs of Work; Proofs of Space.

1. Introduction

Bitcoin, an electronic currency without any physical form, was introduced in 2008 under the pseudonym of Satoshi Nakamoto. Although the author's or authors' identity remains unknown, the term 'bitcoin' refers to the currency unit, while 'Bitcoin' refers to the entire system. Transactions are verified through cryptography and recorded on a public ledger known as a blockchain, which is not subject to government regulation or financial institution control [1]. The creation of new bitcoins is achieved through mining, in which individuals use specialized software to verify transactions and solve complex mathematical problems, and the supply of bitcoins is limited.

Bitcoin stands out from other payment systems based on fiat currency. It offers methods for funding products and services that are quicker, more adaptable, and more creative. As a cryptocurrency, Bitcoin is unique and widely considered the first of its kind [1, 2]. Transactions with Bitcoin are processed over the internet without a central authority or institution to control it. A network of users maintains this decentralized nature.

Consensus algorithms is responsible for keeping the blockchain safe and efficient [3]. It ensures that all nodes agree on the same version of the blockchain. Several consensus methods are available, such as Proofs of Work, Proofs of Stake, Proofs of Space, Delegated Proofs of Stake.

Chia is a cryptocurrency and blockchain platform created in 2018 by Bram Cohen, the inventor of the BitTorrent protocol. Chia is unique among other cryptocurrencies because it uses a different consensus algorithm called "Proofs of Space" instead of the more commonly used "Proofs of Work" algorithm. Proofs of Space and Time uses hard disk space as a resource for mining new coins rather than relying on the computational power of specialized hardware (such as ASICs) like in Proofs of Work [4]. This means that anyone with a regular computer and some available hard drive space can participate in the Chia network and my new coins.

Transactions on a blockchain are secure and verifiable because the blockchain design uses a consensus mechanism among the network's nodes to validate the information. This eliminates the need for intermediaries. The consensus mechanism is a core concept in blockchain that ensures an environment free from tampering, where all nodes agree on a single version of the truth. In a decentralized network, all nodes must agree on the state of the blockchain, making it challenging for an attacker to introduce a tampered block [5].

Bitcoin mining has been a topic of interest for many years now. However, with the entry of governments, energy producers, and dedicated hardware, the dynamics of Bitcoin mining have shifted

away from decentralization. This has gradually placed most mining power in the hands of certain organizations. The network's growth has come with vast energy constantly "wasted" solely to sustain the currency. In response to this tendency, Chia, based on PoSpace, was created to recover decentralization and fairness in the blockchain. This paper compares the characteristics between PoW and PoSpace by analyzing the algorithms and simulating the process of creating a new block and shows PoSpace has unparalleled advantages compared to PoW.

The structure of the paper: Section 2 is the PoW algorithm in Bitcoin. Section 3 is the PoSpace algorithm in Chia. Section 4 discusses the experiment. Section 5 is the conclusion.

2. PoW in Bitcoin

Proof of work involve a scanning process to identify a particular value. This value must start with a specific number of zero bits when hashed using a cryptographic method like SHA-256. The effort required to obtain this value increases exponentially, and a single hash validation can be used to verify the results.

2.1. New blocks

As shown in Figure 1, Bitcoin does this by declaring a nonce in the block. When CPU workload is used to satisfy proof of workload, no block can be changed without re-establishing the entire blockchain.

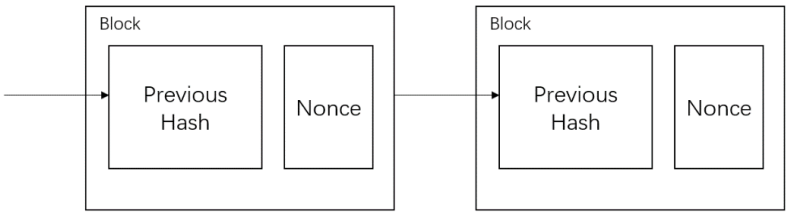

Fig. 1 Bitcoin block chain

The proof-of-work protocol addresses the issue of determining who gets to participate in majority decisions by providing a solution to the challenge of establishing representation. The one-IP-address-one-vote mechanism would be open to manipulation by anyone with access to numerous IP addresses [6]. Proofs-of-work is essentially the one-CPU-one-vote mechanism. The conclusion that is supported by the greatest number of votes is shown by the chain that is the longest and has the most proofs-of-work effort spent in it. The honest chain will outrun other chains and expand the quickest, assuming that honest nodes possess the most CPU power. In order to modify a previous block, an attacker would need to repeat the proof-of-work for the block that came before it as well as all of the blocks that came after it. After that, they would have to play catch-up with the work done by the honest nodes and even outperform it.

2.2. Verification

Payments may be checked by a user without them having to operate a whole network node. In order for them to accomplish this, they will have to keep a copy of the block headers for the proofs that are the longest [2]. The user can obtain this by querying network nodes until they are confident, they have the longest chain. As shown in figure 2, Obtaining the Merkle branch that links the transaction they need to verify to the block where its timestamped is also required. Although the user cannot inspect the transaction directly, they are able to tie it to a specific place in the chain in order to verify whether or not a network node has accepted it. The chain's subsequent blocks provide as additional evidence that the network has approved the transaction.

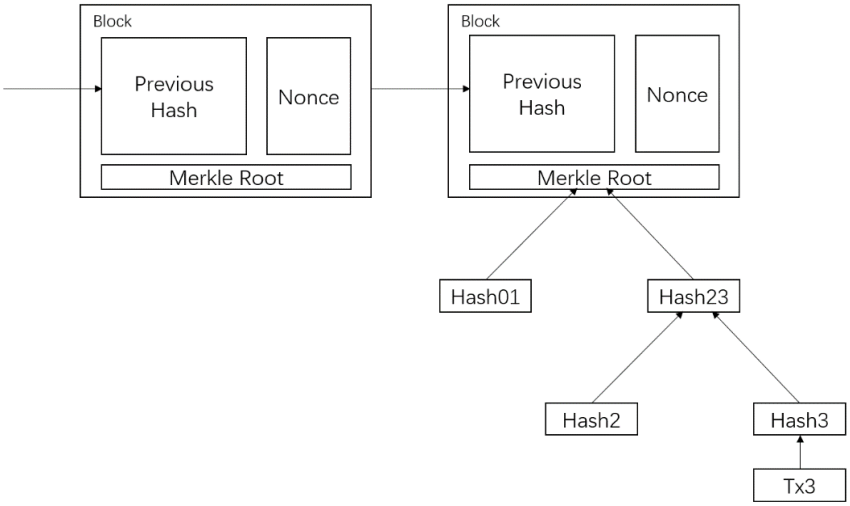

Fig. 2 Bitcoin block chain with Merkle Root

The blockchain is a trustworthy method of payment verification as long as honest nodes are in charge of the network. The verification procedure, however, becomes more prone if an attacker has excessive control over the network. Despite the fact that network nodes are able to verify transactions, a simplified verification technique can be fooled by a dishonest party's bogus transactions as long as the dishonest party can overrun the network [6]. Accepting notifications from network nodes when they identify faulty blocks is one potential fix for this problem. After that, the user's program would be required to download the complete block in addition to the transactions that had been informed, which would validate the difference. Nevertheless, businesses who often accept payments may choose to operate their own nodes in order to provide a higher level of safety and to speed up the verification proces.

3. PoSpace in Chia

3.1. Defination

In a PoSpace protocol, there is a prover P and a verifier V, and in between these two there are two phases. P keeps data F of size N after an initiation step, whereas V holds a little bit of information. When the proof execution step is finished, V might output accept or reject. If P stores F and has random access, V should be very effective in both phases, whereas P should be effective in the execution phase. V, for instance, may be a company that provides free email but demands that customers set aside a sizable quantity of space on the disk, say 100 gigabytes, to stop spam [6]. On rare occasions, V could do a PoSpace to make sure that users have truly set aside the necessary space. In Appendix B, another instance involving online polling is given.

The notation $(outV, outP) \leftarrow hV(inV),\ P(inP)i(in)$ illustrates the execution of an interactive protocol between two parties, P and V, who share an input, in, and have their own local inputs, inP and inV. The input in is shared by both parties [7]. P produces the local output outP while V produces outV. The prover, abbreviated as P, and the verifier, abbreviated as V, are the two interactive random-access machines that make up a proof of space (PoSpace). PoSpace initialization and PoSpace execution are the two stages that make up the PoSpace protocol, and they are both carried out for a statement id that acts as the common input. P cannot utilize the same space more than once for various assertions, thanks to the id. For instance, the id may be the email address itself in the example of an email address from the preceding section.

3.2. Split the chain

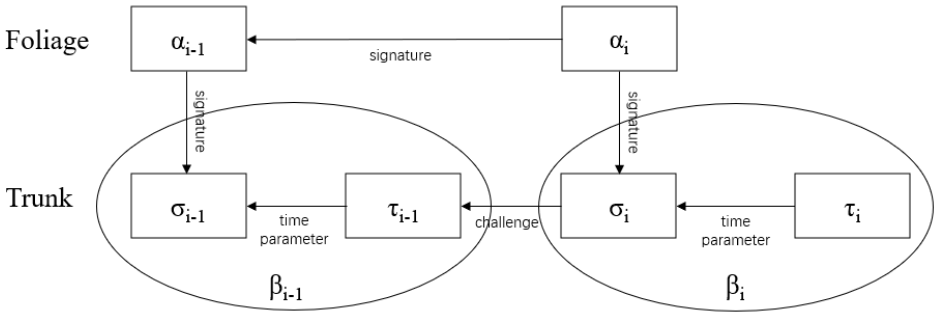

Fig. 3 Divided block chain

As shown in figure 3, Chia is a cryptocurrency that uses a unique two-layered blockchain structure consisting of the Foliage chain (Block α) and the Trunk chain (Block β = (σ, τ)) [8]. The Foliage chain is responsible for storing each block's transactional data and timestamp information. Additionally, it includes the signature of the block that came before it as well as the signature of the evidence of space, which is used to ensure that the miner has allocated a specific quantity of space on the disk to store the Chia blockchain.

On the other hand, the Trunk chain stores the output of proofs of space σ and verifiable delay functions τ (VDFs). The output of the proofs of space ensures that the miner has set aside a particular amount of storage space on the disk, despite the VDFs ensure that the mining process occurs at a predictable and secure rate.

This two-layered structure allows Chia to achieve high security while maintaining scalability. By separating the proofs of space and VDF from the transactional data, Chia can handle a larger number of transactions without sacrificing the network's overall security.

Output of PoSpace. A PoSpace is a proof system that consists of four algorithms [8]: initialization, proving, proof verification, and perfect completeness. The initialization algorithm inputs a space parameter N and a unique identifier pk. It outputs the space S. The proving algorithm, given S and a challenge C as the source of input. The proof verification algorithm takes a proof σ as input and outputs either "accept" or "reject."

$$S = S.\Lambda \leftarrow \text{PoSpace.init}(N, pk) \tag{1}$$

$$\sigma = \sigma.\pi \leftarrow \text{PoSpace.prove}(S, c) \tag{2}$$

$$\text{PoSpace.verify}(\sigma) \in \{\text{reject}, \text{accept}\} \tag{3}$$

$$\Pr[\text{PoSpace.verify}(\sigma) = \text{accept}] = 1 \tag{4}$$

Output of Verifiable delay function. VDF is a cryptographic primitive that takes an input challenge c and a time parameter t as input and generates a proof τ. The VDF.solve algorithm takes these inputs and outputs the proof τ. On the other hand, the VDF.verify algorithm takes the proof τ as input and outputs either accept or reject. The VDF has perfect completeness, meaning that if the proof τ is generated by a valid input and a valid time parameter, the VDF [8]. Verify algorithm will always accept the proof.

$$\tau = \tau.y, \tau.\pi \leftarrow \text{VDF.solve}(c, t) \tag{5}$$

$$\text{VDF.verify}(\tau) \in \{\text{reject}, \text{accept}\} \tag{6}$$

$$\text{VDF.verify}(\text{VDF.solve}(c, t)) = \text{accept} \tag{7}$$

4. Simulation and results

To compare the construction of blockchain networks based on PoW and PoSpace, this paper develops two scripts to simulate the basic operations of Bitcoin and Chia, respectively. These simulations gain practical experience in how these blockchain protocols function and how they differ regarding their underlying algorithms, data structures, and consensus mechanisms. Specifically, PoW blockchains like Bitcoin require miners to solve complex mathematical challenges to verify newly conducted transactions and generate new blocks. In contrast, PoSpace blockchains like Chia rely on the allocation of physical storage space as a means of achieving consensus. By running these scripts and analyzing the resulting blockchains, this paper gains insights into each approach's strengths and weaknesses and how they might be optimized for different use cases and applications.

4.1. Variables controlling

This paper configures the two currencies to have identical chain sizes and difficulty parameters to ensure a fair comparison between the blockchain networks based on PoW and PoSpace. Additionally, to accurately measure the CPU and memory consumption of the programs during runtime, this paper utilizes a profiling tool called VisualVM. To reduce the noise and capture more stable measurements, this paper adds a sleep function of ten seconds to each function call. This ensured that the results captured by VisualVM were more visible and accurately represented the resource consumption of the programs. Specifically, this paper measures each program's CPU usage and memory allocation over the ten-second duration of each function call. These results provide insights into the efficiency and scalability of the respective blockchain protocols and identify potential areas for optimization or improvement.

4.2. System Environment

The computer system features a Core i5-1135G7 CPU and an Iris Xe Graphics 80EUs GPU. The Processor has a 2.4 GHz base clock speed and a maximum 4.2 GHz, while the GPU has 80 execution units. The system is equipped with 16 GB of LPDDR4 memory and a 512 GB SSD for storage.

4.3. Results and analysis

Table 1. Simulation by 3 groups

Sequence	Group Number	1		2		3	
		PoW	PoSpace	PoW	PoSpace	PoW	PosSpace
Testing Parameter	Block Size	108MB		18MB		108MB	
	Difficulty	4		10		18	
Testing Results	CPU usage	1.4%	<1%	10.2%	2.3%	12.4%	3.4%
	Memory usage	48MB	1168MB	153MB	217MB	235MB	1350MB
	Time Comsuming	1003ms	484ms	50102ms	154ms	N/A	492ms

In the first set of tests, the block size was set to 108MB, and the difficulty was set to 4. The results showed that while PoW took twice as long as PoSpace and consumed more CPU resources, its memory usage was only 48MB, compared to 1168MB of PoSpace. This suggests that if memory usage is a limiting factor, PoW might be better than PoSpace. However, if time and CPU resources are more important, PoSpace might be better.

In the second set of tests, the block size was reduced to 18MB, and the difficult parameter was increased to 10. PoSpace takes longer and consumes fewer CPU resources than PoW but uses less time [9].

The third set of tests involved setting both the block size and difficult parameter to relatively large values. In this case, the efficiency of PoW decreased exponentially as the difficulty increased. Besides, its running time was nearly three minutes, so the test had to be stopped manually. This suggests that

while PoW can be more energy-efficient and decentralization than PoSpace under certain conditions, it will exponentially cost system resources when the whole network's computing power increases [10].

5. Conclusion

In conclusion, this paper indicates that PoSpace costs lower CPU/GPU resources but higher storage than PoW. Specifically, for single miners, a Western Digital Red 14TB HDD drive draws 6.5 watts of power under full load, whereas an 8 GPU miner equipped with Nvidia RTX 4090 consumes 3600 watts. Consequently, PoSpace is deemed more energy efficient. Furthermore, for Ethereum, adopting PoS led to a staggering 99.99% reduction in its carbon footprint. PoW mining is predominantly controlled by large-scale mining farms that depend on accessing low-cost electricity to drive a large scale of computing power, resulting in irreversible centralization. In contrast, PoSpace presents a more accessible approach to common people, enabling individuals to participate in the process without specialized hardware. Participants can utilize their computers on the cloud and receive the same payback based on their disk space contribution.

References

[1] Huynh, A.N.Q., Duong, D., Burggraf, T., Luong, H.T.T. and Bui, N.H., 2022. Energy consumption and Bitcoin market. Asia-Pacific Financial Markets, 29(1), pp.79-93.

[2] John, K., O'Hara, M. and Saleh, F., 2022. Bitcoin and beyond. Annual Review of Financial Economics, 14, pp.95-115.

[3] Xie, M., Liu, J., Chen, S. and Lin, M., 2022. A survey on blockchain consensus mechanism: research overview, current advances and future directions. International Journal of Intelligent Computing and Cybernetics, (ahead-of-print).

[4] Shrimali, B. and Patel, H.B., 2022. Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. Journal of King Saud University-Computer and Information Sciences, 34(9), pp.6793-6807.

[5] Xiong, H., Chen, M., Wu, C., Zhao, Y. and Yi, W., 2022. Research on progress of blockchain consensus algorithm: a review on recent progress of blockchain consensus algorithms. Future Internet, 14(2), p.47.

[6] Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. Decentralized business review, p.21260.

[7] Truong, T., 2022. Circular Business Model for Worn Out SSDs Using Proofs of Space and Time (Doctoral dissertation, Worcester Polytechnic Institute).

[8] Cohen, B. and Pietrzak, K., 2019. The chia network blockchain. vol, 1, pp.1-44.

[9] Abusalah, H., SNACKs for Proof-of-Space Blockchains.

[10] Stollenga, M.F., 2022. Embracing Hellman: A Simple Proof-of-Space Search consensus algorithm with stable block times using Logarithmic Embargo. Cryptology ePrint Archive.