Maximizing proof-of-work decentralization

Maximizar la descentralización de la prueba de trabajo

Maximizando a descentralização da prova de trabalho

Davut Çulha[1]

Received: August 15th, 2023
Accepted: November 10th, 2023
Available: January 20th, 2024

How to cite this article:
D. Çulha, "Maximizing Proof-of-Work Decentralization," *Revista Ingeniería Solidaria,* vol. 20, no. 1, 2024.
doi: https://doi.org/10.16925/2357-6014.2024.01.04

Research article. https://doi.org/10.16925/2357-6014.2024.01.04

[1] Aselsan, Ankara. Turkey.
Email: culha@aselsan.com.tr
ORCID: https://orcid.org/0000-0001-5486-1867

Abstract

Introduction: Blockchain technology is one of the emerging technologies that implements the concept of decentralization. The first application of this technology was with Bitcoin, which is a decentralized application. However, the decentralization of Bitcoin has become problematic due to the formation of mining pools. In this work, decentralization is intended to be maximized.

Problem: Decentralization is the main concept of blockchain technologies. However, decentralization suffers mainly from mining pools in the Bitcoin network.

Objective: In this work, the proposed solution to maximize upon the decentralized nature of Bitcoin is to revise the consensus protocol of Bitcoin. The proposed novel consensus protocol called Signature Proof-of-Work uses signatures instead of hashes. The proposed method aims to minimize the number of mining pools and maximize the number of solo miners by arguing that no one can share their private keys with others, which would ensure greater decentralization of the network.

Methodology: The consensus algorithm in Bitcoin is Proof-of-Work. Proof-of-Work allows for the formation of mining pools. Mining pools control the Bitcoin network and reduce decentralization. Therefore, a novel Proof-of-Work consensus algorithm is proposed to empower decentralization.

Results: The proposed consensus algorithm called Signature Proof-of-Work uses signatures instead of hashes. The proposed method aims to minimize the number of mining pools and maximize the number of solo miners by arguing that no one can share their private keys with others, which would ensure greater decentralization of the network.

Conclusion: The proposed consensus algorithm minimizes mining pools by enforcing non-shareable private keys.

Originality: The proposed consensus algorithm is an enhancement of the default Proof-of-Work algorithm of Bitcoin. The proposed algorithm uses signatures instead of hashes, which differentiates it from the default algorithm.

Limitations: In the proposed algorithm, the main argument is that no one shares their private keys. In other words, miners cannot share their private keys with others. If they share their private keys, others can control their own money. Therefore, each miner does not want to collaborate with other miners to mine new blocks. As a result, the mining pools will not be formed.

Keywords: Pool mining, proof-of-work, decentralized consensus, decentralization problems, mining pools, decentralized proof-of-work.

Resumen

Introducción: La tecnología Blockchain es una de las tecnologías emergentes que implementa el concepto de descentralización. La primera aplicación de esta tecnología fue con Bitcoin, que es una aplicación descentralizada. Sin embargo, la descentralización de Bitcoin se ha vuelto problemática debido a la formación de pools de minería. En este trabajo se pretende maximizar la descentralización.

Problema: la descentralización es el concepto principal de las tecnologías blockchain. Sin embargo, la descentralización se ve afectada principalmente por los grupos de minería en la red Bitcoin.

Objetivo: En este trabajo, la solución propuesta para maximizar la naturaleza descentralizada de Bitcoin es revisar el protocolo de consenso de Bitcoin. El novedoso protocolo de consenso propuesto llamado Signature Proof-of-Work utiliza firmas en lugar de hashes. El método propuesto tiene como objetivo minimizar la cantidad de grupos de minería y maximizar la cantidad de mineros individuales argumentando que nadie puede compartir sus claves privadas con otros, lo que garantizaría una mayor descentralización de la red.

Metodología: El algoritmo de consenso en Bitcoin es Prueba de Trabajo. La prueba de trabajo permite la formación de grupos de minería. Los pools de minería controlan la red Bitcoin y reducen la descentralización. Por lo tanto, se propone un nuevo algoritmo de consenso de prueba de trabajo para potenciar la descentralización.

Resultados: El algoritmo de consenso propuesto llamado Prueba de trabajo de firma utiliza firmas en lugar de hashes. El método propuesto tiene como objetivo minimizar la cantidad de grupos de minería y maximizar la cantidad de mineros individuales argumentando que nadie puede compartir sus claves privadas con otros, lo que garantizaría una mayor descentralización de la red.

Conclusión: El algoritmo de consenso propuesto minimiza los grupos de minería al imponer claves privadas que no se pueden compartir.

Originalidad: el algoritmo de consenso propuesto es una mejora del algoritmo de prueba de trabajo predeterminado de Bitcoin. El algoritmo propuesto utiliza firmas en lugar de hashes, lo que lo diferencia del algoritmo predeterminado.

Limitaciones: En el algoritmo propuesto, el argumento principal es que nadie comparte sus claves privadas. En otras palabras, los mineros no pueden compartir sus claves privadas con otros. Si comparten sus claves privadas, otros pueden controlar su propio dinero. Por lo tanto, cada minero no quiere colaborar con otros mineros para extraer nuevos bloques. Como resultado, no se formarán los pools de minería.

Palabras clave: Pool mining, prueba de trabajo, consenso descentralizado, problemas de descentralización, pools de minería, prueba de trabajo descentralizada.

Resumo

Introdução: A tecnologia Blockchain é uma das tecnologias emergentes que implementa o conceito de descentralização. A primeira aplicação desta tecnologia foi com o Bitcoin, que é uma aplicação descentralizada. No entanto, a descentralização do Bitcoin tornou-se problemática devido à formação de pools de mineração. Este trabalho visa maximizar a descentralização.

Problema: A descentralização é o conceito principal das tecnologias blockchain. No entanto, a descentralização é afetada principalmente pelos pools de mineração na rede Bitcoin.

Objetivo: Neste trabalho, a solução proposta para maximizar a natureza descentralizada do Bitcoin é revisar o protocolo de consenso do Bitcoin. O novo protocolo de consenso proposto, denominado Prova de Trabalho de Assinatura, usa assinaturas em vez de hashes. O método proposto visa minimizar o número de pools de mineração e maximizar o número de mineradores individuais, argumentando que ninguém pode compartilhar suas chaves privadas com terceiros, o que garantiria uma maior descentralização da rede.

Metodologia: O algoritmo de consenso no Bitcoin é Prova de Trabalho. A prova de trabalho permite a formação de pools de mineração. Os pools de mineração controlam a rede Bitcoin e reduzem a descentralização. Portanto, um novo algoritmo de consenso de prova de trabalho é proposto para melhorar a descentralização.

Resultados: O algoritmo de consenso proposto denominado Prova de Trabalho de Assinatura usa assinaturas em vez de hashes. O método proposto visa minimizar o número de pools de mineração e maximizar o número de mineradores individuais, argumentando que ninguém pode compartilhar suas chaves privadas com terceiros, o que garantiria uma maior descentralização da rede.

Conclusão: O algoritmo de consenso proposto minimiza os pools de mineração ao impor chaves privadas que não podem ser compartilhadas.

Originalidade: O algoritmo de consenso proposto é uma melhoria no algoritmo de prova de trabalho padrão do Bitcoin. O algoritmo proposto utiliza assinaturas em vez de hashes, o que o diferencia do algoritmo padrão.

e-ISSN 2357-6014 / Vol. 20, no. 1 / january-april 2024 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

Limitações: No algoritmo proposto, o principal argumento é que ninguém compartilha suas chaves privadas. Em outras palavras, os mineradores não podem compartilhar suas chaves privadas com outras pessoas. Se você compartilhar suas chaves privadas, outras pessoas poderão controlar seu próprio dinheiro. Portanto, cada minerador não quer colaborar com outros mineradores para minerar novos blocos. Como resultado, os pools de mineração não serão formados.

Palavras-chave: Pool mining, prova de trabalho, consenso descentralizado, problemas de descentralização, pools de mineração, prova de trabalho descentralizada.

1. INTRODUCTION

Blockchain technology is an emerging technology. There are many implementations of this technology. The first implementation was with Bitcoin [1]. Bitcoin is a reliable system, and it can be considered as the first implemented technology of trust concept. However, this trust system has some drawbacks. The most important drawback is its huge energy consumption. The huge energy consumption is the result of the Bitcoin consensus protocol. A consensus protocol is one of the fundamental technological parts of blockchain systems. A consensus protocol provides trust to the participants of the network by reaching an agreement among the participants without trusting any participant.

Proof-of-Work (PoW) is the consensus protocol of Bitcoin. PoW uses computational power to reach the agreement. As new participants join the Bitcoin network, the total computational power of the network increases. In PoW, computational power is used to solve hash problems. As a result, whenever the revenue of participants is profitable, the total computational power of Bitcoin will increase. Computational power is directly related to energy consumption. In short, energy consumption is a very crucial problem in Bitcoin-like PoW mechanisms.

Blockchain technology can be expressed as a decentralization technology. Trust is the main artefact of blockchain technology. Trust is provided without trusting any participant, but each participant takes a role for the trust. If each participant takes a very little role and each role is equal to other roles, trust will be maximized. This maximization is called decentralization. In other words, decentralization involves maximizing the number of participants and equalizing their individual roles in a network. The opposite of decentralization is centralization. In centralization, trust becomes problematic because a few participants may control the network. Therefore, centralization is another big problem in Bitcoin-like blockchains.

Centralization creates risks to Bitcoin. One of these risks is security. The most notorious security risk for blockchain systems is the so-called "51% attack" or "majority

e-ISSN 2357-6014 / Vol. 20, no. 1 / january-april 2024 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

attack". In other words, if more than 50% of the network becomes centralized, the centralized participants can manipulate the network.

Decentralization should be established. In this work, the Bitcoin PoW mechanism is revised to make it more decentralized. In Bitcoin, miners try to solve PoW puzzles. When one of them solves the puzzle, it is rewarded with money. Miners get rewarded very infrequently as the result of the large number of miners. Therefore, miners form mining pools to increase the reward rate. In other words, miners try to support centralization. To solve this type of centralization, mining pools may be decentralized. Centralization creates powerful miners, which solve PoW puzzles faster. Moreover, they do not announce the solution of PoW puzzles until weak miners are able to solve the puzzles. Therefore, they obtain additional time for solving the next puzzles. This is not fair for the Bitcoin system. Consequently, centralization should be minimized, or decentralization should be maximized for a reliable blockchain system.

The paper is structured as follows. In the following section, related work is summarized. Then, the proposed mining algorithm is explained. Experimental results are given. Lastly, a conclusion is made after a brief discussion.

2. RELATED WORK

An important part of blockchain technology is the consensus protocol, which is the reaching of agreement among blockchain network nodes. There are many consensus protocols. In [2], consensus protocols are surveyed based on PoW. A systematization framework is described to analyse the building blocks of consensus protocol design. Moreover, performance and security properties of the consensus protocols are discussed. In [3], a comprehensive exploration is conducted on the prominent blockchain consensus algorithms. The intricate details of these algorithms are thoroughly discussed, shedding light on their distinct characteristics. Furthermore, a comparative analysis is carried out, focusing on three key aspects: security, limitations, and the degree of decentralization. The paper also provides a concise summary of the strengths and weaknesses associated with each algorithm. Additionally, the paper introduces several enhanced algorithms that have been developed based on these mainstream consensus algorithms.

PoW is used in many blockchains including Bitcoin and the first implementation of Ethereum [4] [5]. PoW depends on computational power, which is used to solve hash problems. PoW is incentivized proportional to the used computational power. Therefore, it encourages energy consumption according to the required computational power.

The biggest problem in PoW is energy consumption. In [6], the Optical Proof of Work (oPoW) consensus algorithm is proposed to reduce energy consumption. oPoW requires special photonic processors which use photons instead of electrons. These processors reduce energy consumption dramatically. In [7], the PoW algorithm is changed to reduce energy consumption. Mining activity is divided into two rounds. In the first round, all the miners compete to be selected to mine the block. In the second round, only selected miners participate in the mining activity. Therefore, energy consumption can be reduced to nearly 50%. In [8], a similar mechanism called Delegated Proof of Work (DPoW) is used to reduce energy consumption. In [9], an alternative algorithm is proposed instead of PoW. The algorithm is called the Register-Deposit-Vote (RDV) algorithm. In RDV, each public key is associated to a MAC address. Therefore, RDV limits the number of nodes in the blockchain network. It makes the blockchain more decentralized. Moreover, there is no mining mechanism, and energy consumption decreases. In [10] [11], the energy consumption of PoW is directed to useful computational tasks instead of reducing energy consumption. In [12], the PoW is accelerated instead of attempting energy reduction. Consequently, it increases the scalability of the blockchain system. In the method, a manager distributes different tasks of PoW to the nodes in the blockchain network. Therefore, each node deals with different tasks in the mining activity. In [13], an energy-efficient consensus mechanism is designed by combining PoW with a consensus mechanism called Proof of Contribution (PoC). In PoC, miners receive difficulty rewards in addition to mining rewards.

The paper [14] presents a novel approach to addressing the energy consumption issue by redefining it as a multi-objective optimization problem. The objectives considered in this formulation include energy consumption, carbon emissions, decentralization, and trust. To tackle this problem, a model consisting of multiple fitness functions is proposed. This model enables the exploration of the intricate search space by identifying a subset of miners that can minimize energy consumption while still preserving the fundamental objectives of blockchain technology.

In [15], an examination is conducted on PoW and its six variants, with a comprehensive analysis of their respective advantages, disadvantages, scalability, maintenance cost, block generation time, transaction cost, energy consumption, validator selection criteria, mining profitability, and susceptibility to a 51% attack. Through thorough investigation and comparison, the study introduces several blockchain consensus algorithms that bear similarities to PoW. These algorithms are then subjected to analysis, and the results reveal that the "dPoW" and "HPoW" algorithms outperform

the others across all parameters. Consequently, they are identified as strong candidates for serving as alternative approaches to PoW in future applications.

In [16], a new consensus protocol is introduced, which builds upon the Proof of Activity protocol and incorporates elements of game theory. This consensus protocol offers notable advantages in terms of energy efficiency and effectively addresses challenges such as selfish mining and majority attacks. Moreover, the protocol enables fast block creation without the need for high-end hardware. An interesting characteristic of this protocol is that it discourages the formation of mining pools among nodes.

Mining pools control a major part of the total computational power in the Bitcoin network. In other words, there are many nodes but most of them are controlled by a few of them, which are mining pools. This is called centralization. Whereas energy cost is the biggest problem in Bitcoin, centralization is the biggest problem according to the spirit of blockchain technology. The spirit of blockchain technology is decentralization, which is the opposite direction of centralization.

In [17], decentralization is analysed. For full decentralization, the number of different actors in the network should be maximized, and the distribution of effective power among the actors should be even. In the realm of blockchain technology, achieving simultaneous implementation of decentralization, scalability, and security poses a significant challenge known as the blockchain trilemma. This well-known problem has prompted the formulation of various approaches and ideas aimed at overcoming it. The paper [18] delves into an investigation of this problem, offering a taxonomy and presenting a comparison of blockchain solutions. The blockchain trilemma is a central issue that hampers the widespread adoption of blockchain across different industries. To gain insights into potential solutions, the paper conducts a systematic literature review, examining popular and conventional approaches publicly available from researchers and developers. These approaches are categorized into first-layer solutions, second-layer solutions, and distributed ledger types, based on the modifications they introduce. The paper provides an analysis of these diverse approaches, highlighting their respective strengths and weaknesses in relation to the trilemma problem. In essence, the selection of a blockchain solution aligned with specific business goals prioritizes one or two aspects of the trilemma, thereby encouraging advancements in those areas.

In [19], the risks of centralization and dishonest administration of mining pools are discussed. The needed tools are highlighted for monitoring the distribution of rewards, authorization and reputation of mining pools, and the development of decentralized pools. In [20], the largest Bitcoin mining pools are analysed. The three to four largest mining pools control more than 50% of the total hashrate. This is a clear

indication of the centralization problem in Bitcoin. In addition to this type of centralization, there is also a second level of centralization in the mining pools. In the three largest mining pools, only a few actors receive over 50% of all Bitcoin rewards. In [6], single points of failure are discussed from a regional point of view. Because of Bitcoin PoW's heavy dependency on electricity, miners are concentrated in regions where electricity prices are low. Changing the PoW algorithm with a photonics PoW algorithm is proposed as a solution to the regional electricity dependency problem.

In [2], selfish mining is discussed. Selfish mining means that a miner withholds solved blocks and begins solving the next blocks before the network. If the network catches up the selfish miner, the selfish miner releases the first of the withheld solved blocks. Centralization increases selfish mining. As a result, selfish miners can realize 51% attacks to the network with only 25% of the total computational power. In [21], selfish mining is analysed. Stronger selfish miners increase their revenue whereas the revenue of honest miners and even weaker selfish miners decreases. As a result, selfish mining increases centralization in return.

In [17], security risks of centralization are evaluated. If more than 50% of the miners or 33% of the effective power are controlled by central authorities, the network can be manipulated by the central authorities. In [22], it is pointed out that 90% of Bitcoin mining power is controlled by 16 miners. In [23], to reduce the security risks of a centralized cloud computing environment, decentralization is used. To develop a general-purpose decentralized computing environment, smart contracts are employed. Most decentralized networks utilize methods of motivation to organize and encourage the involvement and collaboration of peers, thus ensuring the effectiveness and security of the network. In [24], the authors conduct a thorough examination of incentive mechanisms employed in decentralized networks and networked systems. These reviewed mechanisms aim to establish fairness and incentivize participation and cooperative behaviour. The study explores approaches that replace central authority with independent and subjective mechanisms, operating separately at each participating peer, as well as methods that employ multiparty computation. The incentive mechanisms are categorized based on monetary, reputation, and service rewards, allowing for differentiation in their implementations and evaluation of their data management, resistance to attacks, and contribution models. Additionally, the article identifies research gaps and shortcomings in reproducibility and comparability. It is worth noting that the study of incentives in peer-to-peer networks is undergoing rapid development.

A recent research paper [25] introduces a novel consensus protocol aiming to mitigate security risks. The suggested algorithm effectively addresses concerns like unfair miner selection, 51% attacks, forking, and the double spending problem, all while

requiring minimal computational resources. It offers robust protection irrespective of the attacker's hashing power or amount of currency owned. Additionally, the proposed protocol successfully resolves the significant delay encountered in transaction confirmations.

As new miners join the network, the variance of mining profit rises notably. As a result, miners form mining pools because they want to stabilize their profit [22]. In addition to this centralization, there is also geographical centralization [6]. Miners are gathered in regions with low energy costs.

A solution to the centralization problem is decentralized mining pools. In [26], a decentralized mining pool called SMARTPOOL is implemented using Ethereum smart contracts. SMARTPOOL is a decentralized autonomous pool operator program, which provides low profit variance to the miners. In [27], non-outsourceable PoW puzzles are proposed to mitigate centralization. Non-outsourceable puzzles are not suitable for pool mining because mining rewards go directly to the real miners which solve the PoW puzzles. In this work, a novel non-outsourceable PoW mechanism is proposed for decentralization.

In [16], an innovative consensus protocol is presented that combines the Proof of Activity protocol with game theory. The proposed protocol demonstrates notable advantages in terms of energy efficiency and the ability to handle challenges such as selfish mining and majority attacks. Within the paper, a new consensus protocol specifically designed for blockchain networks is introduced. This protocol offers several advantages, including remarkably low energy consumption, a high block creation speed, and the elimination of the need for advanced hardware. Additionally, the protocol discourages the formation of mining pools among nodes.

In [28], a solution to the centralization problem is proposed from the hardware point of view. Traditional PoW algorithms are solved faster by specialized hardware called ASIC. A few firms produce ASIC hardware so that a centralization problem occurs due to the hardware. A kind of PoW algorithm, which is not easy for ASIC hardware, is proposed to mitigate hardware-dependent centralization. In [29], a network of chains called Chainweb is introduced to support decentralization as well as scalability. Chainweb makes PoW parallel by combining many independent PoW chains. Another solution to the centralization problem is individual adjustment of the PoW difficulty according to the computational power of miners [30]. The revised PoW consensus protocol determines different difficulty levels for each miner in the network so that each miner has an equal opportunity to mine new blocks regardless of their computational power. In [31], PoW is changed to mitigate centralization. StrongChain is introduced, which is a revised PoW algorithm where miners collaborate instead of competing.

3. THE PROPOSED MINING ALGORITHM

The proposed mining algorithm uses signature proof-of-work (sPoW) [32]. In sPoW, instead of taking hash of messages, messages are signed and obtained signatures are used. Rewards are directly distributed to the miners' Bitcoin addresses.

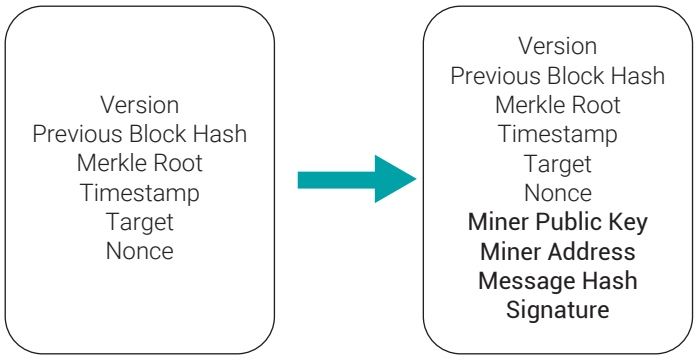

Figure 1. Block header changes
Source: own work

In Figure 1, the left box shows the block header fields of Bitcoin, and the right box shows the block header fields in the proposed algorithm. For sPoW, the following fields are added to the block header: "Miner Public Key", "Miner Address", "Message Hash", and "Signature".

The field "Miner Public Key" is the public key of the miner. The "Miner Address" field is the Bitcoin address calculated directly from the public key of the miner. The rewards will be sent to the "Miner Address". The "Message Hash" field is the SHA256 hash of the Bitcoin's block header plus the fields "Miner Public Key" and "Miner Address".

The first transaction in a block in Bitcoin is called the coinbase transaction. The coinbase transaction is used to distribute mining rewards and transaction fees. In the proposed algorithm, the coinbase transaction is kept unchanged. However, the output addresses should have "Miner Address" value. Therefore, the rewards and fees cannot be sent somewhere else like the mining pool addresses.

In Bitcoin, an Elliptic Curve Digital Signature Algorithm (ECDSA) is used for signing. Especially, the elliptic curve Secp256k1 is used. In the proposed algorithm, again the same curve can be used. When a message is signed with a private key, a signature is produced. Then, the signature can be verified with the public key and the message.

In the proposed algorithm, miners sign the field "Message Hash" with their private keys. They obtain 512-bit signatures. The signature is kept in the "Signature" field. The least significant 256-bit part of the signature is taken as a comparison value.

e-ISSN 2357-6014 / Vol. 20, no. 1 / january-april 2024 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

When one of the miners finds a comparison value less than the field "Target", it adds the block to the Bitcoin blockchain. The other miners in the network accept the newly mined block if the new block ensures the following criteria:

- The comparison value part of the field "Signature" should be less than the field "Target".
- The coinbase transaction should contain the "Miner Address" in the output addresses.
- The field "Miner Address" should be the corresponding address of the field "Miner Public Key".
- The field "Message Hash" should be obtained from the block header fields except the fields "Message Hash" and "Signature".
- The "Signature" field should be verified with the fields "Miner Public Key" and "Message Hash".
- In addition to the above criteria, the Bitcoin block acceptance criteria which does not coincide with the proposed algorithm should be satisfied.

4. EXPERIMENTAL RESULTS

The proposed algorithm is implemented using a Python program, which is run with 25 miners. Each miner is represented as a separate thread within the program. The program continues execution until a total of 2500 blocks are successfully mined in the blockchain. This entire process is repeated four times.

In Table 1, the rows represent the miner numbers, while the columns correspond to the program executions. The table cells display the counts of mined blocks for each combination. Additionally, the last row presents the standard deviation of each execution, with the values being 16.85, 18.60, 16.33, and 16.46, respectively. The average of these standard deviations is calculated to be 17.06.

Table 1. Counts of mined blocks

		EXECUTION 1	EXECUTION 2	EXECUTION 3	EXECUTION 4
MINER NUMBER	1	103	108	75	128
	2	126	123	134	90
	3	105	88	85	103
	4	93	76	123	75
	5	93	100	106	108

(continúa)

e-ISSN 2357-6014 / Vol. 20, no. 1 / january-april 2024 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

(viene)

		EXECUTION 1	EXECUTION 2	EXECUTION 3	EXECUTION 4
MINER NUMBER	**6**	90	85	98	101
	7	93	100	84	90
	8	128	113	79	89
	9	98	116	76	105
	10	105	76	86	80
	11	82	71	123	86
	12	66	103	118	118
	13	106	77	92	85
	14	129	138	78	113
	15	112	107	98	105
	16	103	106	119	74
	17	86	91	97	113
	18	97	123	112	100
	19	87	76	93	127
	20	103	85	88	78
	21	78	112	107	113
	22	98	108	108	90
	23	114	117	115	90
	24	73	126	112	134
	25	132	75	94	105
STANDARD DEVIATION		16.85	18.60	16.33	16.46

Source: own work

5. DISCUSSION

In the proposed algorithm, the main argument is that no one shares their private keys. In other words, miners cannot share their private keys with others. If they share their private keys, others can control their own money. Therefore, each miner does not want to collaborate with other miners to mine new blocks. As a result, the mining pools will not be formed.

The proposed algorithm maximizes decentralization by increasing the number of different miners. In other words, there will be no mining pools because sPoW is a non-outsourceable puzzle. However, there will be miners which have very different computational powers.

The experimental results have an average standard deviation of 17.06. This means that each miner mined blocks approximately between 83 and 117. In other words, all the miners mined blocks near average 100 blocks. Consequently, the network is decentralized.

e-ISSN 2357-6014 / Vol. 20, no. 1 / january-april 2024 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

When the sPoW algorithm is applied in Bitcoin-like blockchains, miners will want to increase its performance. Probably there can be hardware implementations like ASIC in the future. These hardware implementations will calculate ECDSA signatures faster.

6. CONCLUSION

One of the major challenges faced by blockchain technologies is centralization, which poses a significant threat to the underlying philosophy of decentralization. In the context of this study, the focus is on addressing the centralization problem within the Bitcoin PoW consensus mechanism. To achieve this, a revised PoW mechanism, called sPoW, is proposed.

Unlike traditional PoW where hashes play a central role, the sPoW mechanism relies on cryptographic signatures. Miners are required to sign block headers using their private keys in order to obtain specific signature patterns that meet the criteria for successful block mining. By incorporating private keys into the PoW activities, sPoW ensures that miners maintain control over their own mining operations.

By adopting sPoW, the goal is to maximize decentralization in the mining process, and thereby reduce the prevalence of mining pools. Miners are disincentivized from joining mining pools since sharing private keys with others is not feasible or desirable. As a result, individual miners are encouraged to operate independently, leading to a more decentralized network.

In summary, the proposed sPoW mechanism presents a solution to the centralization problem in blockchain technologies, specifically in Bitcoin PoW. By shifting the focus from hashes to signatures and incorporating private keys into the mining process, sPoW aims to maximize decentralization and minimize the reliance on mining pools.

7. REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, vol. 21260, 2008.

[2] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, G. Danezis, SoK: Consensus in the age of blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* (pp. 183-198), 2019.

[3] Y. Xiong, C. Hu, Comparative Research on Blockchain Consensus Algorithms. In *2022 International Conference on Blockchain Technology and Information Security* (ICBCTIS) (pp. 160-164). IEEE, 2022.

[4] A.M. Antonopoulos, *Mastering Bitcoin: Programming the open blockchain*. O'Reilly Media, Inc. 2017.

[5] V. Buterin, *Ethereum white paper*. GitHub repository, 1, 22-23, 2023.

[6] M. Dubrovsky, M. Ball, B. Penkovsky, *Optical proof of work*. arXiv preprint arXiv:1911.05193, 2019.

[7] N. Lasla, L. Alsahan, M. Abdallah, M. Younis, *Green-PoW: An Energy-Efficient Blockchain Proof-of-Work Consensus Algorithm*. arXiv preprint arXiv:2007.04086, 2020.

[8] M. Kara, A. Laouid, A. Bounceur, F. Lalem, M. AlShaikh, R. Kebache, Z. Sayah, A Novel Delegated Proof of Work Consensus Protocol. In *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)* (pp. 1-7). IEEE, 2021.

[9] S. Solat, Rdv: An alternative to proof-of-work and a real decentralized consensus for blockchain. In *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems* (pp. 25-31), 2018.

[10] K. Chatterjee, A.K. Goharshady, A. Pourdamghani, Hybrid mining: exploiting blockchain's computational power for distributed problem solving. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing* (pp. 374-381), 2019.

[11] S. Talukder, R. Vaughn, A Template for Alternative Proof of Work for Cryptocurrencies. In *2021 International Conference on Smart Generation Computing, Communication and Networking* (SMART GENCON) (pp. 1-6). IEEE, 2021.

[12] S. Shahriar Hazari, Q.H. Mahmoud, "Improving transaction speed and scalability of blockchain systems via parallel proof of work," *Future internet*, vol. 12, no. 8, pp. 125, 2020.

[13] T. Xue, Y. Yuan, Z. Ahmed, K. Moniz, G. Cao, C. Wang, Proof of contribution: A modification of proof of work to increase mining efficiency. In *2018 IEEE 42nd annual computer software and applications conference (COMPSAC)* (pp. 636-644). IEEE, 2018.

[14] A. Alofi, M.A. Bokhari, R. Bahsoon, R. Hendley, "Optimizing the Energy Consumption of Blockchain-based Systems Using Evolutionary Algorithms: A New Problem Formulation," *IEEE Transactions on Sustainable Computing*, vol. 7, no. 4, pp. 910-922.

[15] P. Rani, R. Bhambay, A Comparative Survey of Consensus Algorithms Based on Proof of Work. In *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022*, (pp. 261-268). Singapore: Springer Nature Singapore.

[16] Z. Boreiri, A.N. Azad, A novel consensus protocol in blockchain network based on proof of activity protocol and game theory. In *2022 8th International Conference on Web Research (ICWR)* (pp. 82-87). IEEE, 2022.

[17] Y. Kwon, J. Liu, M. Kim, D. Song, Y. Kim, Impossibility of full decentralization in permissionless blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* (pp. 110-123), 2019.

[18] R. Halim, *Decentralization, Scalability, and Security Trade-off in Blockchain System: Comparison on Different Approaches* (Bachelor's thesis, University of Twente), 2022.

[19] I.E. Khairuddin, C. Sas, An Exploration of Bitcoin mining practices: Miners' trust challenges and motivations. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-13), 2019.

[20] M. Romiti, A. Judmayer, A. Zamyatin, B. Haslhofer, *A deep dive into bitcoin mining pools: An empirical analysis of mining shares*. arXiv preprint arXiv:1905.05999.

[21] H. Azimy, A. Ghorbani, Competitive selfish mining. In *2019 17th International Conference on Privacy, Security and Trust (PST)* (pp. 1-8). IEEE. 2019.

[22] S. Chu, S. Wang, *The curses of blockchain decentralization*. arXiv preprint arXiv:1810.02937. 2018.

[23] R. Karanjai, K. Kasichainula, N. Diallo, M. Kaleem, L. Xu, L. Chen, W. Shi, Decentralized Application Infrastructures as Smart Contract Codes. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-9). IEEE. 2022.

[24] C. Ihle, D. Trautwein, M. Schubotz, N. Meuschke, B. Gipp, „Incentive Mechanisms in Peer-to-Peer Networks. A Systematic Literature Review," *ACM Comput. Surv*, vol. 56, no. 1.

[25] A. Endurthi, A. Khare, Two-tiered consensus mechanism based on proof of work and proof of stake. In *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 349-353). IEEE. 2022.

[26] L. Luu, Y. Velner, J. Teutsch, P. Saxena, {SmartPool}: Practical Decentralized Pooled Mining. In *26th USENIX Security Symposium (USENIX Security 17)* (pp. 1409-1426), 2017.

[27] A. Miller, A. Kosba, J. Katz, E. Shi, Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 680-691). 2015.

[28] J. Ding, A new proof of work for blockchain based on random multivariate quadratic equations. *In International Conference on Applied Cryptography and Network Security* (pp. 97-107). Springer, Cham. 2019.

[29] W. Martino, M. Quaintance, S. Popejoy, *Chainweb: A proof-of-work parallel-chain architecture for massive throughput*. Chainweb Whitepaper, 19. 2018.

[30] R. Nakahara, H. Inaba, Proposal of fair proof-of-work system based on rating of user's computing power. In *2018 IEEE 7th global conference on consumer electronics (GCCE)* (pp. 746-748). IEEE.

[31] P. Szalachowski, D. Reijsbergen, I. Homoliak, S. Sun, {StrongChain}: Transparent and Collaborative {Proof-of-Work} Consensus. In *28th USENIX Security Symposium (USENIX Security 19)* (pp. 819-836).

[32] D. Culha, "A random and transaction-positioned blockchain," *Comptes Rendus de l'Academie Bulgare des Sciences*, vol. 73, no. 7, pp. 915-925.