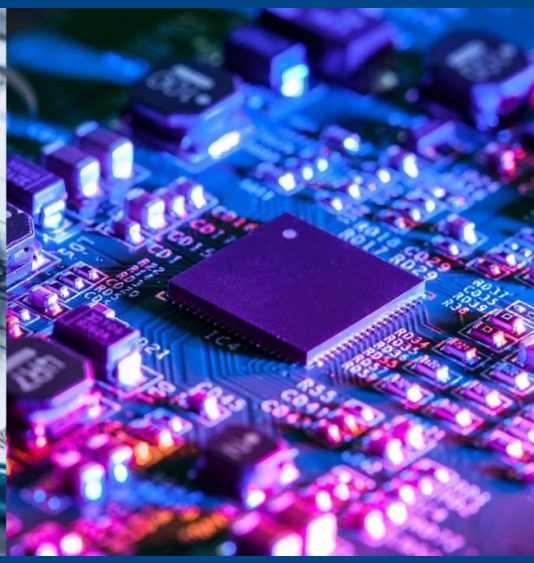
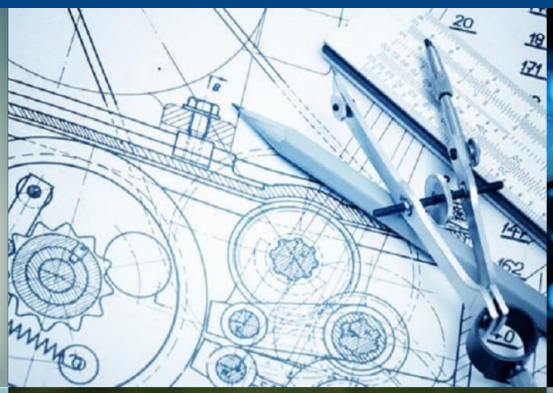
ISSN: 2582-7219

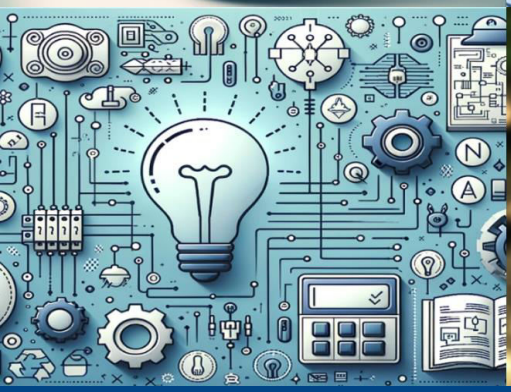




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 6, June 2025**

© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806019

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Enhancing Blockchain Scalability and Transaction Throughput

Clavin Moras

Department of Computer Applications, St. Joseph Engineering College (Autonomous) Vamanjoor, Mangalore, India

ABSTRACT: Blockchain, a distributed ledger technology, forms a distributed consensus on a history of transactions and is the foundational technology for Bitcoin and other cryptocurrencies. Its applications also extend beyond the financial sector. The transaction verification process for cryptocurrencies is slower compared to traditional digital transaction systems. This paper proposes a method to enhance scalability by accelerating the Proof of Work process through parallel mining instead of solo mining. The aim is to prevent multiple miners from duplicating efforts on solving the same block. The proposed method involves selecting a manager and distributing work among miners. The method has been implemented in a test environment and tested with various scenarios by altering the difficulty level and number of validators. Results also show the feasibility of the proposed method.

KEYWORDS: Blockchain, cryptocurrency, proof of work, nonce, transactions, Bitcoin, bitcoin mining.

I. INTRODUCTION

In traditional financial systems, a third party is always required to verify transactions. For instance, when someone wants to buy a product using a credit or debit card, a bank or another financial institution verifies the transaction. Even if cash is used, withdrawing it from the bank involves a third party. Therefore, transactions in conventional systems are centralized through a third party, creating a potential single point of failure. The aim of blockchain technology, which can be either permissionless or permissioned, is to establish a decentralized framework [1].Cryptocurrencies typically use a public or permissionless blockchain, allowing anyone to participate in transactions. On the other hand, permissioned blockchains restrict the validation process to a designated group of participants, which is useful within private organizations or networks. This approach provides a distributed ledger containing the history of all confirmed transactions. It also offers a shared system where users can independently verify the transactions of others without the involvement of a third party. Additionally, blockchain ensures the anonymity of all transactions and user information, while maintaining a continuously growing ledger copy for every system user. However, blockchain technology is not without concerns [2,3]. One significant issue is scalability, particularly the rate at which transactions are processed on the Bitcoin network. Many cryptocurrencies use the blockchain network for transactions, mining, and ledger maintenance, but all face scalability challenges. In contrast, traditional transaction processors like VISA have achieved peak transaction rates of 10,547 transactions per second [4]. The transaction speed varies among cryptocurrencies due to their different protocols. Table 1 illustrates the transaction speed and confirmation time for various cryptocurrencies, adapted from [5].

Table 1: Transaction speed of various cryptocurrencies.

Cryptocurrency	Transaction per Second	Average Transaction Confirmation Time
Bitcoin	3-7	60 min
Ethereum	15-25	6 min
Ripple	1500	4 s
Bitcoin Cash	61	60 min
Stellar	1000	2-5 s

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Litecoin	56	30 min
Monero	4	30 min
IOTA	1500	2 min
Dash	10-28	15 min

A. Mining and Miners

A cryptocurrency needs some sort of system to keep one decision party from manhandling it. A decentralized system has no expert to designate this assignment; hence blockchain set a protocol by which miners need to contribute some work to meet all the requirements for this task [6]. Any individual with the required computation power and processor can be a miner. Fundamentally, there are three obligations of a miner: to verify the transactions; to create a new block containing the transactions; and to immediately verify the block which has been created. To create a new block, miners have to find a hash, which is the result of a cryptographic calculation that interfaces the new block with its antecedent. Subsequent to finding a hash or a solution, a miner can create a block and add it to the blockchain. Other miners then verify the solution. As an impetus, the miner will receive a particular amount of cryptocurrency as a reward. However, the miner should have enough computational power to solve the hash within the time period.

B. Proof of Work

The algorithm that is used to confirm the transaction and add new blocks to the chain is called Proof of Work[8]. With Proof of Work, miners go up against each other to finish exchanges on the system and be compensated. A decentralized ledger accumulates every one of the exchanges into blocks. A block is added to the blockchain when any miner solves the hash for that block.The puzzle consists of many elements such as puzzle protocol and hash function. The complexity of the puzzle increases with the growth of the network. For different types of cryptocurrency, different types of techniques are used as proof of work. For example, Bitcoin uses the SHA-256 cryptography technique [8]. Litecoin also follows a similar type of system, known as scrypt [8] while Ethereum uses the Ethash algorithm [8]. Elements such as transaction time, complexity, and hash power differ in different cryptocurrencies due to dissimilar algorithms.

C. Decentralized System

A decentralized protocol empowers saving assets in a platform that can be found on the Internet. Through a decentralized protocol, the owners have absolute authority over their resources and have the right to exchange assets with anyone at any time [9]. The innovative nature of blockchain has found a way to form a decentralized system in the web. This system will allow owners to process their property any time they want without the participation of a third party. Individuals can specifically enjoy the exchange for a minimum charge. Moreover, a decentralized system such as this has no single point of failure, unlike a centralized system.

II. METHODOLOGY

To perform the proof of work, some of the data used by the miners are identical, including the Bitcoin index, the hash value of the previous block, and the timestamp. However, the content of transactions and the nonce value chosen by the miners may differ. The proposed method is designed in such a way that all miners will use the same transaction data but a different nonce. This means that all miners will use the same data except for the nonce for a certain block, thus ensuring that no multiple miners perform the same work. To provide such an environment, a manager is required to ensure that no two miners use the same nonce value and that all miners use the same transaction data. The manager, who will be chosen from the miners, will be different in every epoch. Here, an epoch contains the time interval between two blocks. In this case, the manager rather than the miner will choose the nonce to compute. In this way, the manager can ensure that no two miners use the same nonce value. The manager is also responsible for creating the transaction hash for a certain block for which s/he is responsible, and which will be provided, along with the nonce value, to the miners. Again, unlike nonces, the transaction hash should be the same for all miners. In a traditional system, all nodes are connected to each other directly or via another node. In the proposed system, they will still be connected to each other and will also be directly connected to the manager. There should be a genesis block at the start of the blockchain with no transactions. While a miner is randomly chosen as the manager for the next block (Block 1), for the remainder of the blocks, the manager selected will be the one who solved the block before the previous block. All the miners will now compete with each other to solve the genesis block, following the traditional method. When the

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

genesis block is solved by a miner, the epoch for the next block will begin. The proposed solution will be effective at this point.

A. Distribution of Data

At the outset, as depicted in Figure 1, the manager will create a transaction hash with the unconfirmed transactions and, at the same time, will generate several groups of nonces. Each group will contain a range of nonce values; no same nonce value should be in multiple groups. If m numbers of miners are active in the network, the manager must initially generate and register at least m number of groups. The manager will then distribute the transaction hash and groups of nonces to each active miner. The system will ensure that no two miners have the same group. With the exception of the manager, all miners will now try to find a solution for the next block with the available transaction data and the range of nonces allocated to each of them.

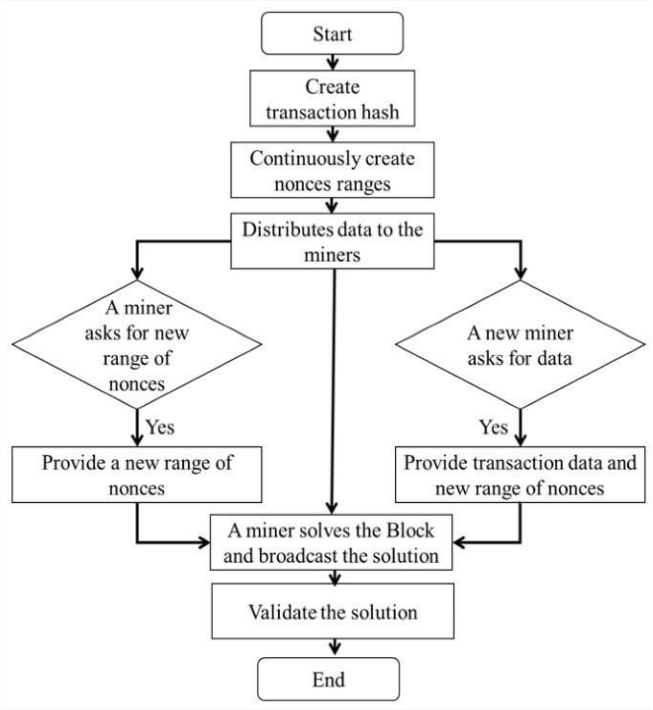


Fig1: Workflow of a miner as a manager.

At the same time, the manager will generate and register more groups of nonces. Once a miner has used all of the nonce values of the allocated range, the miner will ask the manager for a new nonce range. The manager will then provide an unused range to that miner. Again, if a new miner enters into the network and asks the manager for required data, the manager will provide him/her with the same transaction data and a new group of nonces. For this reason, the manager should generate as many groups of nonces as possible. The process will continue until a designated solution for the current nonce is found.

B. Transaction Speed

The goal of parallel mining is to increase the scalability of the system. Through parallel mining, the miner can more quickly reach consensus and so the transaction will be verified sooner. This will be beneficial for the general user who makes the transactions. According to evaluation test results, when compared to solo mining, this method registered a significant improvement.

C. Fairness to the Miners

In this system, every miner has an equal opportunity to be a manager. Furthermore, the reward system is considered in such a way that every contributor to a block (the manager and the miner who solved the hash) can obtain a portion of

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

the reward. In terms of processing power, the miner who invests more in increasing the processing speed will have a higher probability of becoming a manager. Although everyone will work in parallel, the miner with more processing power will have the ability to calculate more nonce value, thus increasing the probability of becoming a manager. Fig 2 and 3 show the block solving and block validation techniques, respectively.

```
1. Initialization
Asks for nonce range and transaction hash to the manager.
Receives transaction hash T from the manager.
Receives nonce range N from the manager.
2. Create record
Record = Sha256 (Block index + Previous block hash + timestamp + T ……)
3. Solve puzzle
for i = initial nonce value to N do
  if length(Blockchain) > new block.index then
        Block already solved
        Validate the Block solution
        Break
  Solution = SHA256(Record+i)
  if Solution satisfies the target then
        Solution found
        Broadcast the solution
        Break
  end if
end for
if solution is not found or Block not already solved then
  Asks for new nonce to the manager
  Receives nonce range N from the manager
  Repeat step 3
end if
```

Fig2: Block solving technique

The current system and the proposed technique increase the probability of a miner with more processing power solving the puzzle. In the current system, it is theoretically possible for the miner with the highest computational power to solve all the blocks in the network. However, this is not allowed in the proposed system. Upon solving a block, in order to receive a reward, a miner has to act as a manager for the subsequent block. This allows for more decentralization in the system.

```
if Previous Block Index+1 != New Block Index
    return false
else if Previous Block Hash != New Block Previous Hash
    return false
else if Hash(New Block) > target
    return false
else
    return true
end if
```

Fig3: Block Validation technique

III. RESULT AND DISCUSSION

Specifically, a peer-to-peer network has been developed by using the GX library of Golang [12]. This is a decentralized package manager that is used to distribute the same program to different nodes. In order to perform the Proof of Work, a SHA-256 cryptographic hash algorithm has been used. The genesis block, which has no transaction record and no previous hash value, has been core coded. The miner who first connects to the system will be the manager for the next block as default.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The test has been conducted based on different numbers of peers, both in solo and parallel mining, using different difficulty levels. Here, the difficulty level denotes the least number of consecutive zeros required at the beginning of an acceptable hash. Figures 6 and 7 represent the test result based on solo and parallel mining. Here, the average time(s) refers to the average time required to solve a block in seconds. This is calculated after conducting several tests under the same conditions and taking the average of all results. To identify the solution, the index, timestamp, transaction hash, previous hash and nonce are taken as input. Here, for the solo mining index, the timestamp and previous hash are the same for a certain block for all miners. In parallel mining along with these data, the transaction hash is also the same for all miners for a certain block.

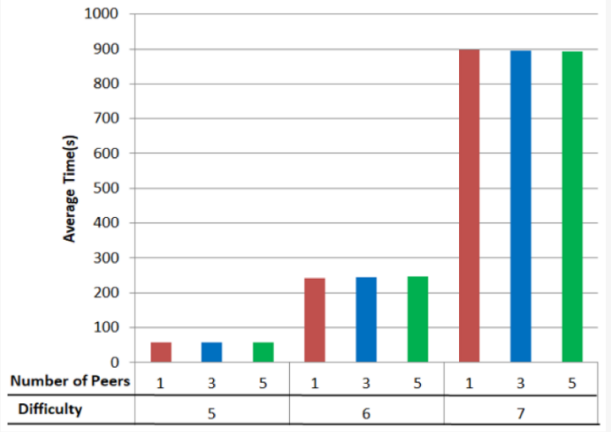


Fig4: Test Results For Solo Mining.

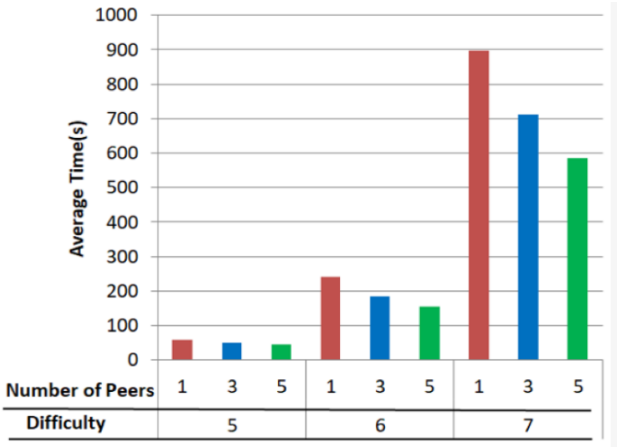


Fig5: Test Results For Parallel Mining.

For difficulty levels 1, 2, 3 and 4, there is no significant difference between solo mining and parallel mining. However, for difficulty levels 5, 6 and 7, there is improvement in parallel mining, and, as Figures 4 and 5 depict, this improvement becomes significant with the increase in the difficulty level and the number of miners. In solo mining, the average time depends only on the level of difficulty, but, in parallel mining, the average time depends on both the difficulty level and the number of peers. If the level of difficulty increases, the average time required increases. Again, if the number of peers increases, the average time decreases because the miners are working in parallel and no two miners perform the same work. Another important aspect to notice is that the average time taken for one peer in parallel mining is almost the same as that in solo mining regardless of the number of peers. This is because, when there is only one miner in parallel mining, no parallel work is taking place. The improvement reaches 34% for five miners compared to one miner. It should be noted that the results may vary based on the processing power allocated to the miners.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

There are several challenges and case scenarios regarding manager, peer and network behavior, One of it is Single Point of Failure In the proposed method, at the beginning of each epoch, all miners have to depend on the manager to obtain a transaction hash and nonces. If the manager goes offline or fails to respond, there can be a single point of failure. However, due to the proposed reward system, this is a very unlikely scenario. Upon fulfilling responsibility as manager, a miner will receive a reward. If unable to fulfill this responsibility, the miner will forfeit the reward as a penalty. The proposed method is designed in such a way that the duration of the single point of failure will remain only for the one epoch where it happens. If a manager fails to respond, the miner can create the transaction hash and can also generate the nonces. In permissionless blockchain systems, every miner has access to all the transaction records. As a result, for that block, the miner will follow the traditional system with a different nonce and a different transaction hash. This type of epoch will take longer as the miners will perform solo rather than parallel mining. However, the next block will again follow the proposed system since the manager has been decided by the previous block.

IV. CONCLUSION

In this paper, we proposed a novel method to enhance the scalability and transaction throughput of blockchain networks by accelerating the Proof of Work process through parallel mining rather than solo mining. The method involves the selection of a manager and the distribution of work to ensure that no more than two miners put the same effort into solving a specific block. Our experimental results demonstrate that the proposed method is feasible and effective in improving the speed and efficiency of transaction processing in blockchain networks. Future work will be focusing on further refining the parallel mining method and exploring its applicability to other blockchain protocols and networks. Additionally, long-term studies on the security and decentralization impacts of this approach are necessary to ensure that it maintains the core principles of blockchain technology while delivering enhanced performance.

REFERENCES

[1] Yli-Huumo, J. (2016). Where is current research on blockchain technology? A systematic review. PLoS ONE, 11, e0163477.
[2] Scherer, M. (2017). Performance and Scalability of Blockchain Networks and Smart Contracts. Umea University: Umea, Sweden.
[3] Joseph, B., Andrew, M., Jeremy, C., Arvind, N., Joshua, A., & Kroll, E. Felten, W. (2015). Research perspectives and challenges for bitcoin and cryptocurrencies. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA.
[4] Cryptocurrency Transaction Speeds: The Complete Review. (2018). The Daily Hodl.
[5] Understanding Cryptocurrency Transaction Speeds. (2018). Coinmonks Medium. Medium.
[6] Nakamoto, Satoshi. (2017). Bitcoin: A Peer-To-Peer Electronic Cash System.
[7] Cong, L.W. (2018). Decentralized Mining in Centralized Pools. SSRN Electron. J.
[8] Types of Cryptocurrency Hashing Algorithms. (2018). Bitcoin Lion Your Gate to Cryptocurrency. Bitcoinlion.Com
[9] Crosby M, Nachiappan P, Pattanayak S, Verma V, & Kalyanaraman (2015). Blockchain Technology. In Sutardja Center for Entrepreneurship & Technology Technical Report Sutardja Center for Entrepreneurship & Technology Berkeley, UC, USA.
[10] Hazari S.S, & Qusay H.M. (2019). A parallel proof of work to improve transaction speed and scalability in blockchain systems. In Proceedings of the IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA.
[11] Hazari, S.S. (2019). Design and Development of a Parallel Proof of Work for Permissionless Blockchain Systems. Master's Thesis, Ontario Tech University, Oshawa, ON, Canada.
[12] Implementation Code for Parallel Mining. (2019). (Accessed on 29 July 2024).

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com