International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 July 2023 **Revised:** 14 September 2023 **Accepted:** 28 September 2023*

Enhancing Transaction Speed of Blockchain System via Parallel Proof of Work

Ms. Priyanka[1], Dr. Hemant Verma[2], Dr. Ritu Makani[3]
[1]Research Scholar, GJUST, Hisar, Haryana
[2]Assistant Professor, Ch. Bansilal University, Bhiwani, Haryana
[3]Associate Professor, GJUST, Hisar, Haryana,
priyankaarora2844@gmail.com, Hemantverma21@gmail.com, ritunagpal1973@gmail.com

Abstract: Blockchain is an online distributed and decentralised ledger system that records transactions and maintains an eternal, verifiable record set of data. While blockchain is employed in many domains, its application in the financial sector is still in its infancy. In this sector, consensus algorithms are used in numerous forms for transaction verification, such as in Bitcoin, Ethereum, Litecoin, etc. Many resources and time are needed for this process. Using concurrent mining instead of solo mining is one way to solve this issue. The main goal of parallel miming is to ensure that the effort required to solve and verify a given block is not shared by more than two processes. In this book, we present several consensus algorithms used to various cryptocurrencies with various blockchain types, explain the bitcoin mining process, and attempt to employ parallel proof of work to accelerate the transaction verification process.
Keywords: Bitcoin, Consensus, Cryptocurrency, mining, proof of work, nonce.

1. Introduction

If we wish to buy something online or in person using a credit or debit card, we must first have the transaction confirmed by a third party, such as a bank or other financial institution, before we can use blockchain technology in the financial sector for money transfers and transaction verification. In case we choose to pay with cash, we must first take out the cash from the bank. This indicates that a third party is engaged in the transaction verification process whether we pay with cash or a card. which has the possibility of failure and where all transactions are managed by a third party. We can create a decentralised network with nodes that are directly connected to one another, akin to a peer-to-peer network, and that doesn't require third parties for verification by employing the Blockchain. The majority of cryptocurrency uses permissioned or public blockchains, which make it simple for anybody to sign up and participate in the network in order to conduct transactions.

All transactions are kept track of by the Blockchain in a ledger called blocks, which are transparent and visible to all parties. Before any transaction is uploaded to the blockchain, it is first confirmed through the mining process. The verification process takes a lot of time and effort in order to add the transaction to the block. whereby system users that remain anonymous keep track of every transaction. Nowadays, the majority of financial systems on the market employ the Blockchain network for ledger maintenance, transactions, and mining. In contrast to standard transaction providers like VISA, which processes 10,547 transactions per second, most cryptocurrencies struggle with scalability and time issues. Depending on their individual protocols, cryptocurrencies vary in their transaction speeds [1]. For a variety of cryptocurrencies, Table 1 shows the transaction speed and confirmation time [2].

Table 1. Transaction Speed of various cryptocurrencies

Cryptocurrency	Transactions per Second	Average Transaction Confirmation Time
Stellar	1000	2–5 s
Ethereum	15–25	6 min
Monero	4	30 min
Bitcoin	3–7	60 min
Ripple	1500	4 s
Litecoin	56	30 min

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 July 2023 **Revised:** 14 September 2023 **Accepted:** 28 September 2023*

Dash	10-28	15 min
IOTA	1500	2 min
Bitcoin Cash	61	60 min

1.1 Features of Cryptocurrency:

Cryptocurrency is used world-wide and accepted almost everywhere because of some features, these are:

1. **Secure:** wherein the blockchain transactions are encrypted using a variety of robust cryptographic techniques. To eliminate any possibility of failure or vulnerability, every transaction is recorded in a distributed ledger called Blockchain. Because information is held on a distributed network, which increases the security of bitcoin, all transactions become less susceptible to mistakes, system failures, and hacking.

2. **Fast and Global:** All transactions in cryptocurrency are instantaneously confirmed and spread over a distributed network, regardless of their physical locations.

3. **Divisibility**: Bitcoin can be further divided into smaller pieces, known as Satoshi. This is one way that cryptocurrency can be further divided. The bitcoin unit is minuscule. A Bitcoin comprised of 100 million Satoshi units.

4. **No permission required:** It is not necessary to obtain permission from anyone in order to exchange cryptocurrencies. Direct free software downloads are made by the user node, which also trades money with other nodes.

5. **Efficient:** The bitcoin trade is just as efficient as sending money via a bank transfer. Third parties are not required for the confirmation and verification of the transfer. Consensus algorithms, one type of blockchain protocol, automatically validate transactions, improving efficiency.

6. **Irreversible and immutable:** Transactions cannot be altered or reversed once they are stored in a block. Transactions are impossible to modify thanks to a variety of encryption techniques. where each node is connected to the others and modifications made to one affect the hash of the next node. If the transaction data is changed, we can quickly identify the modified node.

7. Anonymous: When exchanging money or processing transactions, users' identities are kept secret or anonymous from other users in the system since a central authority is not necessary. After being verified and validated by a distributed, decentralised network, new transactions are entered into the blockchain.

2. Miners and mining:

A blockchain-based financial system requires some kind of mechanism to decide whether to validate and verify transactions because transaction verification does not involve a third party. This validation and verification were carried out by kids. A certain type of node known as a "minor" has enormous processing power and a sizable amount of memory for storing transactional data. Minor essentially completes three primary tasks: quickly verifies the produced block, creates a new block containing the transaction, and verifies all of the transactions. The process by which nodes referred to as "minors" in the context of Bitcoin or "forgers" in the context of Ethereum verify new transactions and add them to the blockchain ledger is known as mining. Youngsters or counterfeiters compete to find the solution to a challenging mathematical puzzle based on a cryptographic hash algorithm—basically, hashing and nonce.

It is desirable for the hash value to be less than the goal value. A hashed block header must be less than the target value in order for a new block to be given. If the hash does not equal the target value or is less than it, the minor must increment the nonce and return the hash. This procedure is repeated numerous times until the required hash is produced. Upon finding the solution, the new block is propagated and added to the network. A nonce's value ranges from 0 to 4,294,967,296.

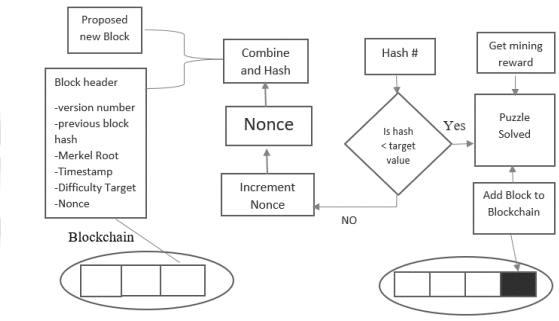

Fig.1 Mining Process

A difficult mathematical challenge that requires a lot of time, effort, and computing power is solved by smaller nodes competing with one another. The first minor to produce the winning hash will receive transaction fees or extra bitcoins. Initially, the reward for finishing this mining task was 50 Bitcoins. These days, the award is 12.5 bitcoins, valued at $125,000 [3]. Every four years, the amount will drop by half.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 July 2023 **Revised:** 14 September 2023 **Accepted:** 28 September 2023*

The amount of Bitcoins determines how much the prize is worth. However, hardware costs and electricity usage will eventually increase along. This hash computation technique, known as the consensus process, upholds the blockchain's integrity. Without a consensus method in place, when blocks are added to a blockchain, the

3. Consensus Protocols in Blockchain:

Blockchain technology employs consensus techniques to ensure that all transactions are verified before being added to the blockchain, so "consensus or agreement between the nodes on the network on the status of Blockchain" is required. All transactions on the blockchain are secure and verifiable even in the absence of a central authority. Only the different consensus mechanisms found in blockchain, which are a crucial component of any blockchain network, make this feasible. In a distributed network, we use this type of consensus to achieve stability in the Blockchain Network and to build trust among anonymous peer nodes. By obtaining consent from every other node in the network, consensus makes sure that new nodes can only be added to the blockchain. Therefore, in the context of Blockchain, a consensus protocol is a collection of rules and a procedure that allows involved nodes to concur on the network's present state.

3.1 Various Consensus protocols used in Cryptocurrency:

1. Proof of Work: Developed by Satoshi Nakamoto, pow is the most popular consensus algorithm that was employed on the original Bitcoin Blockchain in 2009. wherein a number of children who are recognised as distributed ledger nodes compete to solve a challenging mathematical puzzle using a cryptographic hash technique. Proof of Work, or POW, is the name given to the determined solution. The mining node distributes the proof of work for verification to the other nodes in order to reach consensus. The network can validate the problem's solution even when it is difficult to come up with. POW's primary objective is to identify the best workable solution to a challenging mathematical problem. Mining is an incredibly computationally demanding activity. Therefore, the first young person to successfully construct the POW will receive payment in digital cash or in the form of Bitcoins. Different cryptocurrencies employ distinct methods as POW. The SHA-256 cryptographic algorithm is used by the Bitcoin coin. [4] A similar process called Scrypt is also used by Litecoin [4]. Ethash is the algorithm used by Ethereum [4].

Disadvantages:

1. Time consuming: Minors undergo a time-consuming series of intricate procedures to arrive at the correct solution, which requires them to repeat the iteration process numerous times.

2. High Energy consumption: Minors carry out a variety of tasks that call for electricity and processing power in order to arrive at the best solution. Just one young person who solves the problem first receives a reward; the other children do not, and their efforts are squandered.

2.Proof of Stake: In contrast to PoW, PoS requires less processing power and energy and does not require sophisticated computations to mine. Rather, the subsequent block is chosen at random according to the node's wealth or stake; the larger the stake, the greater the possibility of mining a block. The more one invests in the validating node, the less likely one is to try to manipulate the validation process. Stated differently, the individuals with the greatest stake in the network will be more motivated to safeguard and maintain it, as any intrusion would reduce the worth and standing of the cryptocurrency they possess. Delegates, forgers, and validators are alternative terms used to refer to mining nodes. A stack of bitcoins must be committed by the delegate into the Blockchain-based network as collateral. The percentage stake that each node has provided determines which node will serve as the forger, and this determination is made using a variety of ways. As an example, 10% of the network stack can be owned by a node, and 10% of transactions can be approved by it. Peercoin, Black Coin, and NXT blockchains all use the Proof-of-Stake mechanism. Ethereum leverages an established PoW Blockchain and a hybrid PoW/PoS method to implement PoS.

Disadvantages:

1. Cheaper to attack: PoS-based networks are easily compromised since an attacker just needs to pay a small sum of money as opposed to needing to invest in hardware, time, money, electricity, and other resources.

2. Centralized Risk: The richest forger has complete control over the consensus-building process and has the potential to get increasingly richer.

3. **Proof of Elapsed Time:** PoET was originally utilised by Intel in 2016. Permissioned blockchain networks use it essentially as a means of selecting the network's block winner. The concept is based on the notion of a fair lottery system where each node inside the network has an equal probability of winning. Each node waits for an arbitrary amount of time before adding proof of their delay to the block. To provide a random wait time, a trustworthy function generates a randomised timer object that is transmitted to each minor node in the Blockchain Network. In order to deter minors from trying to obtain a timer with a shorter duration, this randomization mechanism was employed. Following the designated waiting period, the minor adds a new block to the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 July 2023 **Revised:** 14 September 2023 **Accepted:** 28 September 2023*

blockchain and broadcasts the relevant data throughout the blockchain network. This process is repeated for each newly created node. This approach is less power-hungry and more efficient than proof-of-work (PoW) because it requires less processing power. PoET consensus is leveraged by Intel's Hyperledger Sawtooth architecture.

4. Proof of Authority: The PoA consensus method was proposed in 2017 and is mostly used in private blockchains. It's similar to decentralised proof of stake (PoS) and distributed proof of stake (DPoS) in that only a predefined group of authority known as validators protect the Blockchain and add new blocks. The identities of the validators are available to the public and can be independently checked because it is a public notary database. PoA does not require node-to-node data transfer and consumes minimal energy.

To find validators, a few requirements must be fulfilled:

1. The validators' identities must correspond with the information in the open notary database and be made publicly available.
2. Every validator should be treated equally and consistently by the authority.
3. To ensure that the validator is legitimate, there must be stringent qualifying standards for staking identity.

Hyperledger and Ripple use optimized version of PoA.

The Proof of Stack Anonymous (PoSA), Leased Proof of Stake (LPoS), Proof of Importance (Pol), Proof of Storage, Proof of Burn, Proof of Activity, and other consensus techniques are also utilised.

4. Method of proposed Solution:

The timestamp, the hash of the previous block, and the Bitcoin Index are examples of data sets that are same for all purposes and different for the application of consensus procedures or sophisticated computations like Proof of Work (PoW). Certain data are different, like the transaction content and the nonce value. When employing this suggested technique, every node completes distinct tasks in parallel on distinct nonces inside the same transaction, speeding up computation compared to solo mining.

A manager oversees all of these duties; in order to prevent two nodes from using the same transaction data and performing the same operation on the same nonce value, the management divides the nonce value among all the nodes. With every period, the manager will be unique. Epoch is used to store the time interval between blocks in this case. In this manner, no two minors execute operations on the same nonce value, or each minor executes an operation on a separate nonce value. A manager's duties also include dividing up the nonce and creating the transaction hash for a given block. In lone mining, every node is connected to every other node either directly or indirectly through the use of intermediary nodes. In concurrent mining, every node has the option of having a direct connection to the block manager or to each other.

4.1 Distribution of Data

The manager creates the transaction hash and divides the grouped nonce, as we have discussed, and then distributes this information to all of the minors. The number of nonce groups is equal to the number of minors, and the formation of nonce groups is dependent upon the minor population. All minors will receive a total of m nonce groups, which will be produced if there are m minor nodes. It requires the system to make sure that two minors cannot receive the same set of nonce.

Upon obtaining the nonce group from each minor, attempt to come up with a solution for the next new block utilising the transaction data that is currently accessible and the nonce value that the manager has assigned them. New nonce groups will be generated and registered by the manager at that point. Minors request new nonce values from the manager for additional verification after testing every nonce value. The manager will then provide the minors with a new, unallocated range of nonce. The manager will give the new minor all of these details if, during this validation, the minor enters the network and asks for the same transaction data, hash value, and new group of nonces.

Creating as many new groups as possible and allocating them to the minors is the manager's primary responsibility. Until we arrive at the ideal answer, this verification process will keep going.

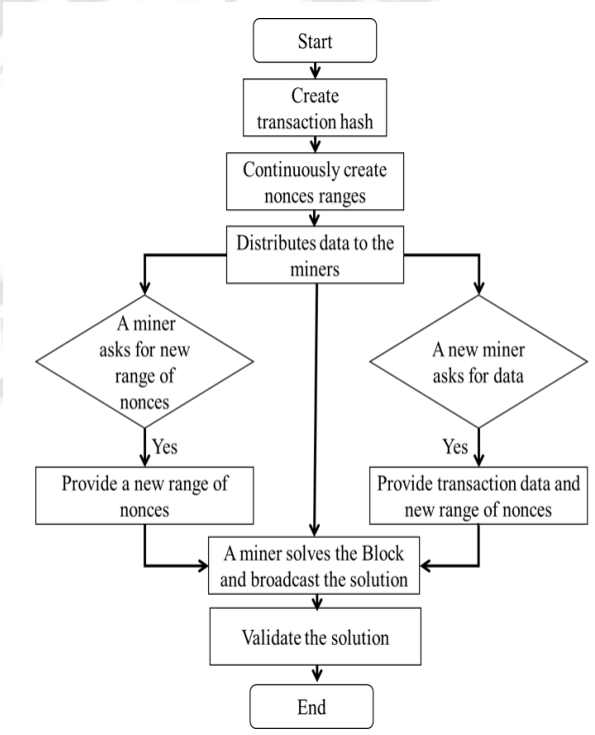

Fig.2 Working of manager

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 July 2023 **Revised:** 14 September 2023 **Accepted:** 28 September 2023*

4.2 Transaction speed:
Maximizing the current system's scalability is the primary goal of the suggested approach. As opposed to solo mining, parallel mining allows all of the minors to work on separate groups of nonces, arrive at a consensus solution more rapidly, and verify transactions more swiftly. Compared to the old mining procedure, this approach will yield a huge improvement.

4.3 Reward System:
The minor who figures out the consensus solution and completes the difficult computation in the previously employed solo mining method receives some mining coins and a transaction fee. The manager who creates the traction and nonce groups and the minor who solves the challenge will split the entire fee under the proposed parallel mining approach. a transaction fee and mining coin in which the minor receives thirty-five percent and the manager receives sixty-five percent.

4.4 Block Solving and Block validation techniques:
Managers and minors complete this work. wherein every minor is given the same chance to advance to manager and take charge of every aspect of parallel mining. The minor and manager receive incentives in the form of mining coins and transaction fees for solving and verifying the block. In this method, several minors work concurrently on various nonce groups, and the more quickly a minor can solve a problem, the greater the likelihood of solving and validating the block. Block validation is represented by Algorithm 2 and block solving by Algorithm 1.

Algorithm 1: Block Solving technique

Step1: Initialization
Firstly, minors ask to manager for transaction hash and nonce range.
Manager gives transaction hash H to minors.
Manager gives nonce range R to minors.
Step2: Create Record
Record=SHA256(Hash of previous Block +Block index value+ Timestamp+ T+……...)
Step3: Solve Puzzle
Apply loop
for i = initialize nonce value to R do
if length (Blockchain)>new block. Index **then**
Block was solved already
Only validate the solution of Block
Break
Solution = SHA256(Record + i)
if Solution satisfies the target, **then**
Solution found successfully
break
end if
end for
If the solution not found or Block not found already then
Asks the new nonce to the manger
Receives nonce range R from the manager
Repeat Step 3
end if

Algorithm 2. Block validation technique

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

4.5 Difference Between Pool mining and Parallel mining

Attribute	**Pool Mining**	**Parallel Mining**
Centralization	For providing the resources to the minors there is central coordinator who is responsible for this task.	In which manager manage the mining process, nonce generation and keep the system Decentralized. No central coordinator is available here.
Rewards	For validation task minor receives rewards based on their contribution in validating process.	Rewards does not split in parallel mining. Mining reward only received by the minor who solve the Block and transaction fee is divided to manager and minor.
Pool Fee	In which the central coordinator takes participant fee and small amount of rewards from every minor.	No reward fee and participant fee are taken by the minors.

Work of Coordinator / Manager	Assignment Distribution and reward splitting, verify the contribution of participant is done by coordinator.	Transaction Hash and Nonce distribution to minors is done by manager.

5. Some Challenges may arise in Proposed method:

5.1 New peers: A new minor always asks the manager for the transaction hash and nonce when they join the network. The transaction hash and nonce group that were not previously allocated are provided by the manager. Managers are unaware of the extent to which minors collaborate on a given transfer. The manager consistently creates and registers the nonce group for any new minors or any existing minors who check the nonce group that was previously assigned.

5.2 Peer leaves the Network: Any minor has the freedom to quit the network whenever they choose. It is feasible that the nonce assigned to a minor who departs the network in the middle of processing provides a solution to the issue, allowing the block to have several solutions for distinct nonce groups. It's feasible that another minor will discover the answer using a different nonce group, and the network won't be affected if a peer departs in between.

5.3 Malicious Manger: It's possible that a manager provides the nonce group that has already been utilised in an attempt to harm a miner. However, before being delivered to minors, the manager is required to register the nonce value in the system, therefore this cannot occur. The already-used nonce group cannot be used again without authorization from the system. Consequently, a manager cannot possibly hurt a minor.

5.4 Single Point of failure: All minors in parallel mining initially rely on the manager for the transaction hash and nonce group. There is only one point of failure if the manager is unresponsive or disappears. At that point, any other minor may fulfil the manager's duties and get the rewards. Should the kid fail to fulfil their manager's responsibilities, they will forfeit their awards as a penalty.

6. **Statement and Declaration:**

- **Compliance with Ethical Standards:** The ethical guidelines for conducting research with human beings were followed in the conduct of this study. There were no animal participants in this investigation. Every participant gave their informed consent, and the study was conducted with full respect for their privacy and confidentiality. There are no disclosed conflicts of interest by the authors that could have impacted the research.
- **Research Data Policy and Data availability Statement:** This article contains all of the data created or analysed during this investigation. The study used to compile the data for this manuscript was supported by a number of research publications, which are included in the references section. After publication, this information will be available to scholars solely for research purposes and on the journal's home page.
- **Competing Interests:** We attest that we have no connection to, or involvement with, any group or entity that has a stake in the topics or information covered in the text, either financially or non-financially. This manuscript used SimBlock to describe the simulation results of a blockchain network.

7 Conclusion and Future Work:

We have covered bitcoin and consensus algorithms in this paper. By dividing the nonce value among minors for the same transition, we suggested a novel approach to parallel mining that would speed up transactions. Our suggested approach speeds up the validation process by introducing the Proof of Work with parallel mining, in which several minors work on a single transition. We have spoken over the several issues that could come up with the suggested approach and how much they would affect the network. Using classifier techniques based on simulation results, we will attempt to implement and assess the suggested method in the future with various features.

Reference:

1. Cryptocurrency Transaction Speeds: The Complete Review. The Daily Hodl. 2018. Available online: https://dailyhodl.com/2018/04/27/cryptocurrency-transaction-speeds-the-complete-review (accessed on 3 November 2018).
2. Understanding Cryptocurrency Transaction Speeds—Coinmonks—Medium. Medium. 2018. Available online: https://medium.com/coinmonks/understanding-cryptocurrency-transaction-speeds-f9731fd93cb3 (accesse on 12 June 2020).
3. David Easley, D., O'Hara, M. and Basu, S., 2019. From mining to markets: The evolution of bitcoin transaction fees. Journal of Financial Economics, 134(1), pp.91–109.
4. Types of Cryptocurrencies Hashing Algorithms—Bitcoinlion.Com. Bitcoin Lion—Your Gate to Cryptocurrency. 2018. Available online: http://www.bitcoinlion.com/cryptocurrency-mining-hash-algorithms (accessed on 5 June 2020).
5. Yli-Huumo, J. Where is current research on blockchain technology? —A systematic review. PLoS ONE 2016,11, e0163477. [CrossRef] [PubMed]
6. Scherer, M. Performance and Scalability of Blockchain Networks and Smart Contracts; Umea University: Umea, Sweden, 2017; Available online:

http://www.diva-portal.org/smash/get/diva2:1111497/FULLTEXT01.pdf (accessed on 15 May 2020).

7. Joseph, B.; Andrew, M.; Jeremy, C.; Arvind, N.; Joshua, A.; Kroll, E.; Felten,W. Research perspectives and challenges for bitcoin and cryptocurrencies. In Proceedings of the IEEE Symposium on Security and Privacy,San Jose, CA, USA, 17–21 May 2015.
8. Cryptocurrency Transaction Speeds: The Complete Review. The Daily Hodl. 2018. Available online: https://dailyhodl.com/2018/04/27/cryptocurrency-transaction-speeds-the-complete-review (accessed on 3 November 2018).