A

Seminar Report On

Cooperative Mining System to Improve Bitcoin Scalability

Submitted in partial fulfilment of the

Requirements for the award of the Degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

(COMPUTER SCIENCE)

By

S Mithilesh Reddy [Reg. No: 23001D5114]

Under the guidance of

Dr. A. ANANDA RAO B. Sc., B. Tech., M. Tech., Ph. D (IIT M)

Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY
ANANTAPUR COLLEGE OF ENGINEERING (AUTONOMOUS)
ANANTHAPURAMU – 515002

ANDHRA PRADESH

2024

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY ANANTAPUR COLLEGE OF ENGINEERING (AUTONOMOUS) ANANTHAPURAMU-515002 DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

Certified that this is a bona fide record of the Technical seminar report entitled,

"Cooperative Mining System to Improve Bitcoin Scalability" done by

S MITHILESH REDDY [Reg. No: 23001D5114]

is submitted to the faculty of Computer Science and Engineering, in partial fulfilment of the requirements for the award of degree of **MASTER of TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING with Specialization of CS (Computer Science)** from Jawaharlal Nehru Technological University College of Engineering (Autonomous), Ananthapuramu during the second semester of academic year **2023-2025.**

Signature of Seminar Coordinator

Dr. A. ANANDA RAO, B. Sc., B. Tech., M. Tech., Ph.D(IIT M)

Professor
Department of CSE
JNTUACEA, Ananthapuramu

Signature of Head of the Department

Dr. K.F BHARATHI, M. Tech., Ph.D.

Associate Professor & H.O.D
Department of CSE
JNTUACEA, Ananthapuramu

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Bitcoin's scalability issues significantly hinder its transaction processing capability, resulting in increased latency and network congestion. This paper introduces a Cooperative Mining System (CMS) designed to address these challenges. CMS allows miners to collaborate on block creation, forming 'super-blocks' that reduce validation time and enhance transaction throughput. The proposed system maintains Bitcoin's core principles of security and decentralization. Extensive simulations and performance evaluations demonstrate that CMS significantly outperforms traditional mining methods, offering a viable solution to Bitcoin's scalability problems. This research underscores the potential of cooperative strategies in improving the efficiency of blockchain networks.

Keywords: Bitcoin, scalability, Cooperative Mining System, blockchain, transaction throughput, network latency, decentralized networks

1.INTRODUCTION

Bitcoin, introduced by Satoshi Nakamoto in 2008, revolutionized digital currency by removing the need for a central authority. Its decentralized nature relies on a distributed ledger, the blockchain, which securely and transparently records all transactions. This innovation has influenced numerous other cryptocurrencies and blockchain applications.

As Bitcoin's popularity grew, the network faced significant scalability issues. The blockchain's limited transaction processing capacity led to higher fees and delays. These challenges stem from Bitcoin's design, which prioritizes security and decentralization over scalability. Various solutions, such as second-layer protocols and core blockchain improvements, have been proposed to address these issues.

One promising solution is the implementation of cooperative mining systems. Cooperative mining allows miners to pool resources and share rewards, enhancing network efficiency, reducing energy consumption, and improving reward distribution.

This report explores cooperative mining systems in detail. We begin with a literature survey on the evolution of Bitcoin mining and cooperative mining proposals. We then provide an overview of cooperative mining principles and benefits. The report covers system architecture and the mining process, highlighting key components and mechanisms for efficient cooperation. We also discuss the advantages, challenges, and potential applications of cooperative mining. Finally, we conclude with a discussion on the future scope and potential impact of cooperative mining on the Bitcoin network.

By leveraging cooperative mining systems, we can address critical scalability challenges in Bitcoin and other blockchain networks. This report aims to provide a comprehensive analysis of cooperative mining and its potential to enhance decentralized network performance and sustainability.

2.LITERATURE SURVEY

2.1 Early Bitcoin Mining Bitcoin mining began with individuals using personal computers. Initially, the network difficulty was low, allowing anyone with a computer to participate. Miners competed individually to solve cryptographic puzzles and validate transactions, earning rewards in newly minted bitcoins.

2.2 Evolution of Mining Hardware As Bitcoin gained popularity, mining difficulty increased, prompting the need for more efficient hardware. The transition from CPUs to GPUs provided a significant boost in processing power. Further advancements led to the development of FPGAs and ASICs, which are specialized for mining and offer superior efficiency. This progression, however, raised concerns about centralization, as advanced hardware became expensive and less accessible.

2.3 Mining Pools To address rising difficulty and resource demands, miners formed pools, combining their computational power to improve their chances of solving puzzles. Mining pools distribute rewards based on each member's contribution, providing more stable and predictable income. This collaborative approach transformed mining, making it more accessible and reducing the risk for individual miners.

2.4 Cooperative Mining Proposals Recent research has focused on decentralized and federated mining systems to enhance cooperation. Decentralized mining pools eliminate the need for a central coordinator, reducing centralization risks. Federated mining systems involve multiple independent entities working together to validate transactions and create blocks, enhancing network security and fairness. These cooperative mining models aim to address Bitcoin's scalability and security challenges, offering a promising path for future improvements.

3.COOPERATIVE MINING SYSTEM (CMS)

The Cooperative Mining System (CMS) proposed by D. Elwi et al. is designed to improve the scalability of Bitcoin. It is divided into four stages: initialization, waiting, integration, and rewarding.

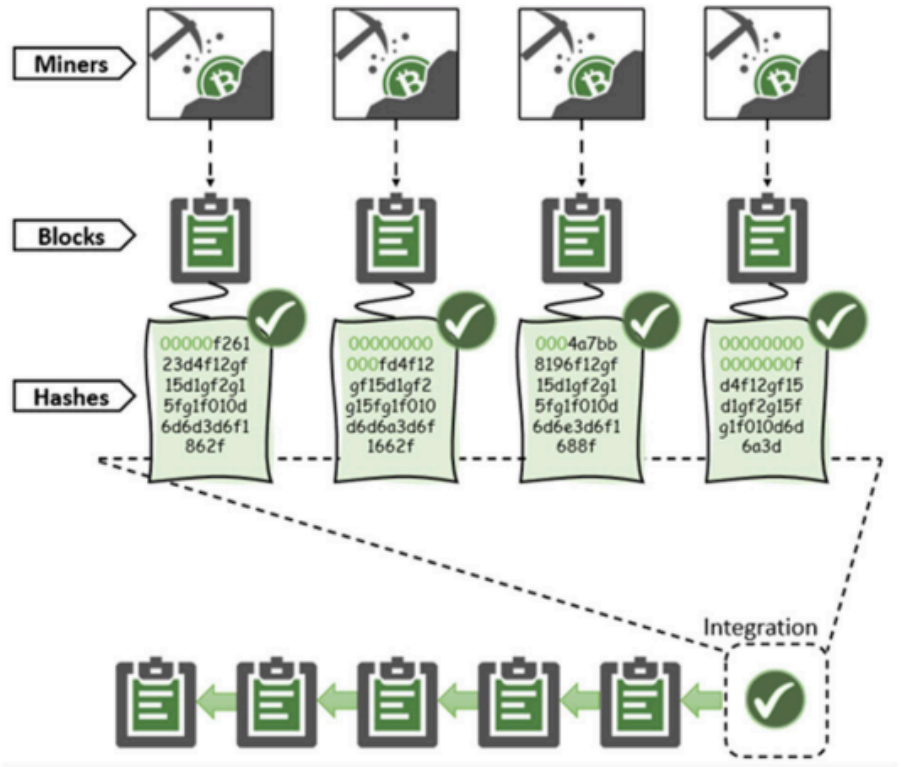

Fig. 3.1 Cooperative Mining System Architecture

1. Initialization

- **Transaction Selection:** Miners individually select transactions from the MemPool to form new blocks. The number of transactions selected depends on the block size, similar to Bitcoin.
- **No Initial Proof of Work (PoW):** Miners create blocks without performing the computationally intensive PoW. This step is a major departure from traditional Bitcoin mining, where PoW is required to create a valid block.
- **Broadcasting Blocks:** After creating these blocks, miners broadcast them to the network. This means that all miners share their selected transactions with each other.

- **Eliminating Competition:** By not requiring PoW at this stage, the CMS removes the competitive aspect of mining. Every block created by a miner is considered useful and will contribute to the final super-block.

2. Waiting

- **PoW Implementation:** After broadcasting their blocks, miners perform PoW on their individual blocks. This step ensures that the blocks meet certain security and validity requirements.
- **Receiving Blocks:** Miners wait to receive blocks from all other participating miners. This ensures that every miner has the complete set of blocks to work with.
- **Controlled Waiting Duration:** The waiting period is controlled by the difficulty level, which adjusts based on the number of miners, network bandwidth, and the hash rates of the miners. This mechanism is similar to Bitcoin, where difficulty adjusts to maintain a consistent block time.

3. Integration

- **Creating the Super-Block:** Each miner individually creates a large super-block. This super-block is a combination of all the transactions from the received blocks.
    - **No Repetition:** Transactions are arranged by their hash numbers to avoid repetition.
    - **Uniformity:** Every miner creates the same super-block because they all have the same set of transactions, ensuring consistency across the blockchain.
- **Ensuring Consistency:** By creating identical super-blocks, all miners maintain the same copy of the blockchain, which helps in achieving consensus without conflicts.

4. Rewarding

- **Equal Rewards:** Unlike traditional mining where the first miner to solve the PoW gets the reward, in the CMS, all participating miners share the rewards equally.
    - **Cryptocurrency Reward:** The reward consists of a certain amount of cryptocurrency, currently 6.25 BTC in Bitcoin.
    - **Transaction Fees:** Miners also share the transaction fees collected from the transactions included in the blocks.

- **Increased Throughput:** Because all blocks contribute to the super-block, the number of transactions processed per unit time increases, improving the throughput of the system.
- **Enhanced Miner Revenues:** With increased transaction throughput, the overall revenue for miners is likely to increase, making the system more profitable for participants.

Key Benefits of CMS

1. **Scalability:** By allowing all blocks to contribute to the final super-block, CMS significantly increases the number of transactions processed, addressing one of Bitcoin's major scalability issues.
2. **Energy Efficiency:** Since PoW is performed only after the initial block creation and sharing, CMS reduces the overall energy consumption compared to the traditional Bitcoin mining process.
3. **Fairness:** The reward distribution is more equitable, as all participating miners share the rewards, unlike the winner-takes-all model in Bitcoin.
4. **Consistency and Security:** By ensuring that all miners create the same super-block, CMS maintains consistency and security across the network.

4.CMS Implementation

Implementing the Cooperative Mining System (CMS) involves creating a framework where miners work together rather than competing against each other. This collaborative approach aims to enhance transaction throughput and reduce latency, addressing scalability issues present in traditional Bitcoin mining. Below is a detailed guide on the implementation process:

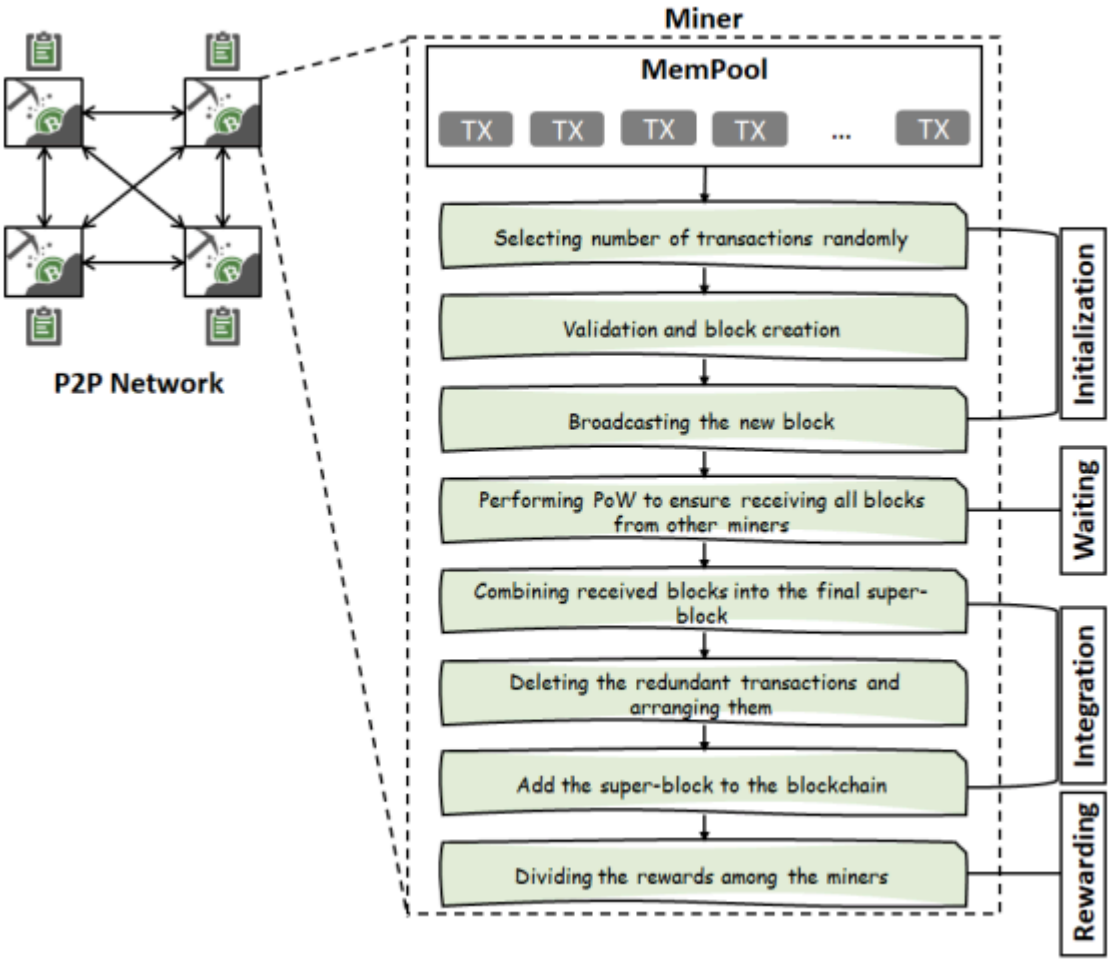

Fig. 4.1 Workflow of CMS

1. System Setup

- **Environment Preparation:** Set up a distributed network of nodes (miners) participating in CMS. Configure each node with the necessary software and network connectivity.
- **MemPool Initialization:** Initialize the MemPool on each node, which holds the transactions awaiting confirmation.

2. Block Creation

- **Transaction Selection:** Each miner independently selects random transactions from the MemPool based on the block size.
- **Initial Block Creation:** Miners create new blocks without performing Proof of Work (PoW) at this stage, containing the selected transactions, and prepare them for broadcasting.

3. Block Broadcasting

- **Broadcasting Blocks:** Each miner broadcasts their newly created block to the rest of the network, ensuring all miners have access to the transactions selected by others.

4. Proof of Work (PoW)

- **Implementing PoW:** After broadcasting, miners perform PoW on their individual blocks, ensuring validity and security.
- **Waiting for Blocks:** Miners wait to receive blocks from all other miners in the network. This waiting period is controlled by the difficulty level, which adjusts based on network size, bandwidth, and hash rates.

5. Integration of Blocks

- **Creating Super-Block:** Each miner creates a super-block by integrating all received blocks, containing all unique transactions arranged by their hash numbers.
    - **Removing Redundancy:** Remove any redundant transactions to ensure each transaction appears only once in the super-block.
    - **Sorting Transactions:** Sort transactions based on their hash numbers for consistency.
- **Consistency Check:** Ensure each miner's super-block matches those created by others, maintaining a uniform blockchain state across the network.

6. Reward Distribution

- **Equal Reward Sharing:** Once the super-block is created, the rewards (both the block reward and transaction fees) are distributed equally among all participating miners.

- **Reward Calculation:** The reward amount, currently set at 6.25 BTC in Bitcoin, along with transaction fees, is divided equally among all miners.

7. Security Measures

- **Handling Miner Malfunction:** If a miner fails to send a block, other miners ignore the disrupted miner and continue the process. The disrupted miner can rejoin the network by reloading the blockchain from active miners.
- **Addressing Block Loss:** In case of block loss, forks may appear. Miners resolve this by re-synchronizing during the next epoch, ensuring consistency.
- **Preventing Blockchain Altering:** CMS maintains the immutability of the blockchain by linking each block to its predecessor using cryptographic hashes, making altering any block computationally expensive.
- **Preventing Double Spending:** CMS uses the distributed blockchain and PoW consensus to prevent double spending, ensuring only one of the conflicting transactions is valid.
- **Mitigating Selfish Mining:** The creation of the super-block depends on all miners, preventing any single miner from hiding blocks for selfish gains.

5.Evaluation and Results

Implementation and Evaluation Results

The simulation of the proposed Cooperative Mining System (CMS), Parallel Mining System (PMS), and Bitcoin Solo Mining System (SMS) was developed using C# .NET programming language. These three systems were implemented on the same real peer-to-peer network to compare them. The network was constructed from devices of different capabilities to ensure that miners were different. Additionally, a server was created to broadcast run commands to all devices, ensuring that all devices started mining simultaneously.

Evaluation Metrics and Parameters

The experiments were conducted on each of the three systems based on three different parameters: the number of peers (miners competing or cooperating to create the new block), the number of transactions (transactions in MemPool waiting for confirmation), and difficulty level (degree of mining difficulty). The system evaluation criteria were average Block Creation Time (BCT), transaction throughput, and transaction latency.

Experiments

Number of Peers

The number of waiting transactions was set to 100, and the difficulty level to 4. The number of peers was varied between 2 to 12 to obtain different scenarios for the mining process. The resulting values for BCT, transaction throughput, and transaction latency in the three systems were observed.

- **Average BCT:** In CMS, the average BCT increases with the number of peers because the number of blocks aggregated to create the super-block increases, leading to longer aggregation times. In PMS and SMS, average BCT decreases as the number of peers increases due to higher hash rates allowing faster block creation.
- **Transaction Throughput:** In all systems, transaction throughput increases with the number of peers. In CMS, all peers create blocks, so the number of transactions increases with more peers. In PMS and SMS, faster block creation due to more peers increases transactions per second.

- **Transaction Latency:** In CMS, latency decreases as more transactions are added to the blockchain. In PMS and SMS, the latency is not significantly affected by the number of peers.

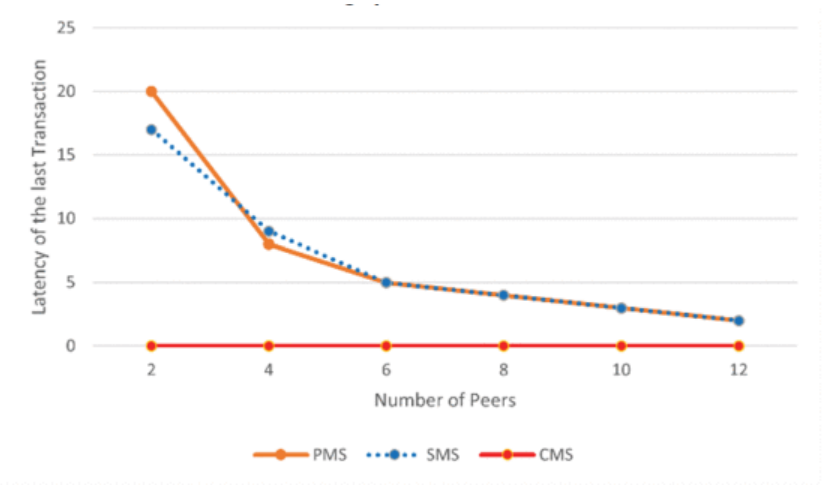

Fig. 5.1 Last transaction latency in minutes for CMS, SMS, and PMS with number of peers.

Number of Transactions

The impact of varying the number of transactions in MemPool was also studied. The results showed that:

- **Throughput**: It is not affected by the number of transactions waiting in MemPool in any of the systems.
- **Latency**: Increasing the number of transactions in MemPool causes longer waiting times until transactions are added to the blockchain in all systems. However, in CMS, this waiting time remains minimal.

Difficulty Level

Different difficulty levels (3, 4, and 5) were used to evaluate the systems with constant numbers of peers and transactions. The findings were:

- **Throughput:** In SMS and PMS, throughput decreases with higher difficulty levels due to increased average BCT. In CMS, throughput remains almost constant.
- **Latency:** In SMS and PMS, latency increases with higher difficulty levels due to decreased throughput. In CMS, latency remains nearly non-existent.

- **Average BCT:** In SMS and PMS, average BCT increases with higher difficulty levels, but in CMS, it remains almost constant because PoW is automatically stopped once all miners receive blocks from other miners.

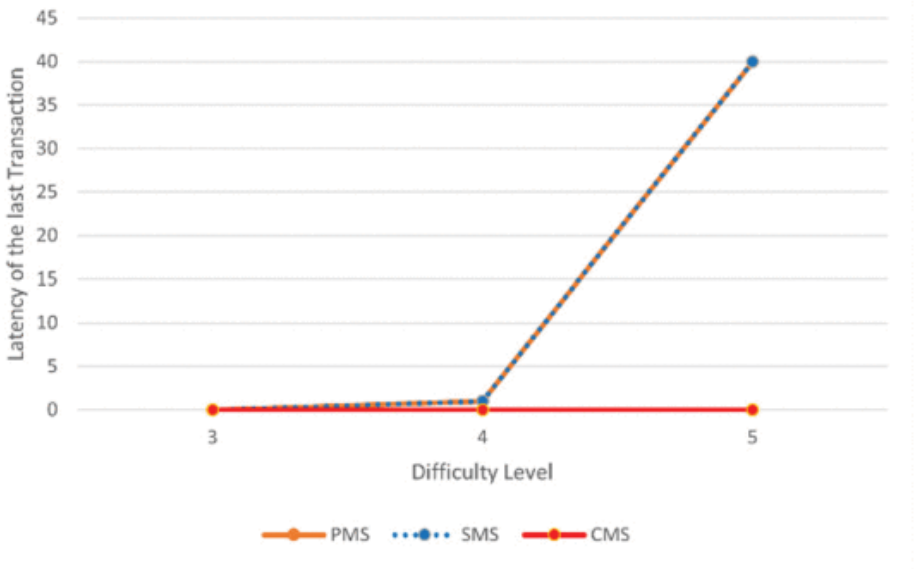

Fig. 5.2 Last transaction latency in minutes for CMS, SMS, and PMS.

Results Discussion

The increase in the number of peers:

- Increases transaction throughput in CMS because all blocks are integrated and added to the blockchain. There are no ignored blocks, leading to M×BSM \times BSM×BS transactions being added every epoch.
- Does not affect transaction throughput in PMS and SMS significantly, as only one block is added per epoch.
- Decreases latency in CMS because the number of transactions added to the blockchain increases, reducing waiting times.
- Does not affect latency significantly in PMS and SMS.

Overall, the proposed CMS significantly increases transaction throughput compared to PMS and SMS, with almost eliminated transaction latency due to high throughput. In contrast, PMS and SMS suffer from confirmation delays.

6.Applications of Cooperative Mining System (CMS)

The Cooperative Mining System (CMS) has significant applications in the realm of blockchain technology, particularly in enhancing the scalability and efficiency of Bitcoin. By allowing miners to cooperate in the creation of blocks rather than compete, CMS significantly increases transaction throughput and reduces latency, addressing key limitations of traditional mining approaches.

Key Applications:

- **Improved Transaction Throughput:** CMS enables multiple miners to create blocks simultaneously and aggregate them into a super-block, thus significantly increasing the number of transactions processed per second. This is crucial for scaling Bitcoin to handle a larger volume of transactions efficiently.
- **Reduction of Transaction Latency:** By integrating blocks created by all miners into a super-block, CMS effectively eliminates transaction delays and starvation, ensuring that transactions are confirmed much faster compared to traditional methods.
- **Decentralization and Security Maintenance:** While improving scalability, CMS also maintains the decentralization and security levels inherent in the traditional Bitcoin system. This ensures that the network remains robust against attacks and continues to operate in a trustless environment.
- **Enhanced Miner Rewards:** The increased throughput and efficiency of CMS lead to higher revenues for miners. As more transactions are processed in a given period, miners receive more transaction fees, making mining more profitable and sustainable.
- **Potential for Cloud Implementation:** CMS can be implemented in cloud environments, such as Amazon EC2, to further increase the network's size and capacity. This approach can help manage the growing size of the blockchain by storing only the latest state of users, rather than the entire transaction history.

By addressing these critical areas, CMS offers a comprehensive solution to the scalability challenges faced by Bitcoin and other blockchain-based systems, paving the way for broader adoption and more efficient operation.

7.Limitations of Cooperative Mining System (CMS)

While the Cooperative Mining System (CMS) presents several advantages in terms of scalability and transaction throughput for Bitcoin, it also has its limitations. These constraints must be considered for a comprehensive understanding of the system's capabilities and areas that need further development.

Key Limitations:

1. **Storage Limitation:**
    - **Blockchain Size:** Miners need to store the complete blockchain to retrieve historical activities, search transactions, and validate new transactions. Over time, the blockchain's size will become enormous, which poses a challenge for miners with limited storage capacities. This may lead to a more centralized network as miners with inadequate storage capabilities are forced to quit.
2. **Aggregation Time:**
    - **Block Aggregation:** The time required to aggregate blocks into a super-block increases with the number of participating miners. This can lead to increased average Block Creation Time(BCT) as the system scales up with more miners.
3. **Difficulty Level Impact:**
    - **Varying Difficulty Levels:** The CMS system, like traditional systems, experiences changes in transaction throughput and latency with varying difficulty levels. Higher difficulty levels may result in increased average BCT, affecting the overall performance and efficiency of the mining process.
4. **Latency with High Transaction Volume:**
    - **MemPool Transactions:** When there is a high number of transactions waiting in the MemPool, even CMS experiences increased latency. Although CMS manages this better than traditional systems, the waiting time for transactions to be added to the blockchain can still grow with higher transaction volumes.
5. **Cloud Implementation Challenges:**
    - **Scalability in Cloud:** Implementing CMS in cloud environments like Amazon EC2 to increase the network's size involves complex challenges. Managing the rapidly growing size of the blockchain and ensuring efficient data structures that store only the latest state of users, are critical areas that need further research and development.

8.FUTURE SCOPE

The future development of the Cooperative Mining System (CMS) holds significant potential for further enhancing blockchain technology, particularly in terms of scalability and efficiency. One of the primary directions for future work is the implementation of CMS in cloud environments such as Amazon EC2. By leveraging cloud infrastructure, the network size can be significantly increased, allowing for more extensive and robust cooperative mining operations. This scalability is crucial for handling the growing volume of transactions as blockchain technology continues to gain widespread adoption.

Another critical aspect of future development is addressing the challenge posed by the rapidly increasing size of the blockchain. As transaction throughput increases, so does the size of the blockchain, making it difficult for miners to store the entire blockchain on their local machines. To mitigate this issue, a change in the blockchain's data structure is proposed. Instead of storing all historical transactions, the blockchain could be designed to store only the latest state of users. This approach would drastically reduce the storage requirements for miners, making it more feasible for a broader range of participants to engage in mining activities without being hindered by storage limitations.

Additionally, future work could involve the development of a scheduler that selects transactions randomly. This innovation would help in distributing the transaction load more evenly across the network, preventing bottlenecks and ensuring a more efficient processing of transactions. A random transaction scheduler could also enhance the security of the system by making it harder for malicious actors to predict and target specific transactions.

9.CONCLUSION

In this paper, we focus on solving the scalability problem of Bitcoin without compromising its decentralization and security, addressing the blockchain trilemma. The Cooperative Mining System (CMS) is proposed as a solution to enhance Bitcoin's scalability in terms of transaction throughput and latency. Unlike the traditional competitive mining approach, CMS introduces a cooperative mechanism where miners work together without dependence, sharing rewards equally. This approach significantly boosts transaction throughput and nearly eliminates transaction delays and starvation issues observed in the traditional Bitcoin system. The improvements are achieved by modifying the proof of work algorithm, with mathematical proofs supporting the enhancements.

Future work will involve implementing CMS in cloud environments like Amazon EC2 to expand network size. Additionally, solutions to address the growing blockchain size, such as altering the data structure to store only the latest state of users, are proposed. Finally, the development of a scheduler that randomly selects transactions is suggested to further optimize the system's efficiency and security

10.REFERENCES

D. Elwi, O. Abu-Elnasr, A. S. Tolba and S. Elmougy, "Cooperative Mining System to Improve Bitcoin Scalability," in IEEE Access, vol. 11, pp. 58715-58728, 2023, doi: 10.1109/ACCESS.2023.3283928.

S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", Decentralized Bus. Rev., no. 2022, pp. 21260, 2008, [online] Available: https://bitcoin.org/bitcoin.pdf. (2008)

Bitcoin, 2022, [online] Available: https://bitcoin.org/en/ (2022)

Ethereum, 2022, [online] Available: https://ethereum.org/en/ (2022)

Iota, 2022, [online] Available: https://www.iota.org/ (2022)

Bitcoin Cash, 2022, [online] Available: https://www.bitcoincash.org/ (2022)

Cardano, 2022, [online] Available: https://cardano.org/ (2022)

Litecoin, 2022, [online] Available: https://litecoin.org/ (2022)

Monero, 2022, [online] Available: https://www.getmonero.org/ (2022)

Neo, 2022, [online] Available: https://neo.org/ (2022)

E. Duffield and D. Diaz, Dash: A payments-focused cryptocurrency, 2018, [online] Available: https://github.com/dashpay/dash/wiki/Whitepaper. (2018)

CoinMarketCap, 2022, [online] Available: https://coinmarketcap.com/ (2022)