Bachelor of Science in Computer Science & Engineering

A Public Blockchain Scheme for Cryptocurrency with an Efficient Consensus Algorithm

by

Suvadra Barua

ID: 1504025

Department of Computer Science & Engineering

Chittagong University of Engineering & Technology (CUET)

Chattogram-4349, Bangladesh.

May, 2021

A Public Blockchain Scheme for Cryptocurrency with an Efficient Consensus Algorithm

Submitted in partial fulfilment of the requirements for
Degree of Bachelor of Science
in Computer Science & Engineering

by

Suvadra Barua
ID: 1504025

Supervised by

Dr. Md. Mokammel Haque
Professor
Department of Computer Science & Engineering

Chittagong University of Engineering & Technology (CUET)
Chattogram-4349, Bangladesh.

The thesis titled '**A Public Blockchain Scheme for Cryptocurrency with an Efficient Consensus Algorithm'** submitted by ID: 1504025, Session 2019-2020 has been accepted as satisfactory in fulfilment of the requirement for the degree of Bachelor of Science in Computer Science & Engineering to be awarded by the Chittagong University of Engineering & Technology (CUET).

Board of Examiners

Chairman

Dr. Md. Mokammel Haque
Professor
Department of Computer Science & Engineering
Chittagong University of Engineering & Technology (CUET)

Member (Ex-Officio)

Dr. Md. Mokammel Haque
Professor & Head
Department of Computer Science & Engineering
Chittagong University of Engineering & Technology (CUET)

Member (External)

Dr. Asaduzzaman
Professor
Department of Computer Science & Engineering
Chittagong University of Engineering & Technology (CUET)

Declaration of Originality

This is to certify that I am the sole author of this thesis and that neither any part of this thesis nor the whole of the thesis has been submitted for a degree to any other institution.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. I am also aware that if any infringement of anyone's copyright is found, whether intentional or otherwise, I may be subject to legal and disciplinary action determined by Dept. of CSE, CUET.

I hereby assign every rights in the copyright of this thesis work to Dept. of CSE, CUET, who shall be the owner of the copyright of this work and any reproduction or use in any form or by any means whatsoever is prohibited without the consent of Dept. of CSE, CUET.

Signature of the candidate

Date:

Acknowledgements

It would not have been possible to complete this thesis work without the support of several people. Professionally and personally, it has been a gratifying experience. Much of what I've accomplished has become possible only because of such monitoring and assistance.

First and foremost, I would like to express my heartfelt gratitude, Professor Md. Mokammel Haque, Ph.D., Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, for his unwavering support and trust in my work during the research. I am grateful for his constant guidance and insightful questions, which have pushed me to think outside of my comfort zone and given me the confidence to take on tasks I never felt I could handle.

My family and my friends deserve praise for their courage in bearing with me during this ordeal. Their unwavering loyalty and inspiration have helped me in every part of my thesis work.

Abstract

With the growing popularity of blockchain technologies, the blockchain platform is experiencing lack of scalability and increasing size issues, causing it inefficient rather than a centralized platform.In the recent years, researches are being conducted to resolve the issues.The beacon chain and shard chain concept of ethereum 2.0 makes their blockchain system scalable. But the problem arises on the point of storage optimization.On the other hand, the mini-blockchain scheme can optimize the storage of each node on the network but it is not scalable.This thesis proposes a 'Mini-Shard Chain' architecture and associated algorithm, 'Proof-of-Duty,'. The research extends scalability and reduces the operating nodes storage requirements. Furthermore, unlike other consensus algorithms, 'Proof-of-Duty' eliminates double-spending, forking, 51% attack and other unfair properties that decreases blockchain security.

Table of Contents

List of Figures

List of Abbreviations

MSC Mini-Shard Chain. 21

PCLB Previous Chain Last Added Block. 19

Chapter 1

Introduction

1.1 Introduction

1.1.1 Block

A block stores data, metadata and most importantly previous block hash. The data and metadata vary from platform to platform. In cryptocurrency, a block contains a list of the most recent transactions that have not yet been stored in any previous blocks. So, a block is similar to a page of a ledger in cryptocurrency. It is permanent storage of documents that can't be changed or removed once they've been written. A block consists of two part,the block header and the block body.

The components of a bitcoin block are shown below:

- **Height:** Current length of the blockchain
- **Virtual Size:** A transaction's weighted size under segwit's rules
- **Block version:** indicates which set of block validation rules to follow.
- **Parent block hash:** A fixed size hash value that points to the previous block.
- **Merkle tree root hash:** The hash value of all the transactions in the block.
- **Timestamp:** Current timestamp as seconds since 1970-01-01T00:00 UTC
- **nBits:** Current hashing target in a compact format.
- **Nonce:**A 4-byte area that normally begins with 0 and increases with each hash measurement.

- **Difficulty:** A measure of how difficult it is to mine a Bitcoin block
- **Body of the Block:**Composed of a transaction counter and transactions.

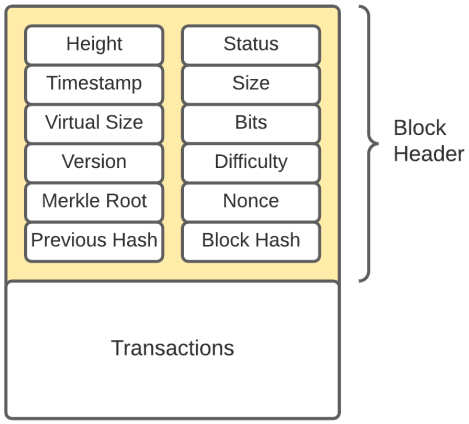

Figure 1.1: A Block of Bitcoin Blockchain

The maximum number of transactions that a block can store depends on the block size and transaction size. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions.

1.1.2 Blockchain

Blockchain is a chain of blocks where each block holds a previous block hash. It is a method of storing data in such a way that it is difficult or impossible to alter or hack. The blockchain is an undeniably brilliant innovation – the brainchild of Satoshi Nakamoto, an individual or group of people.

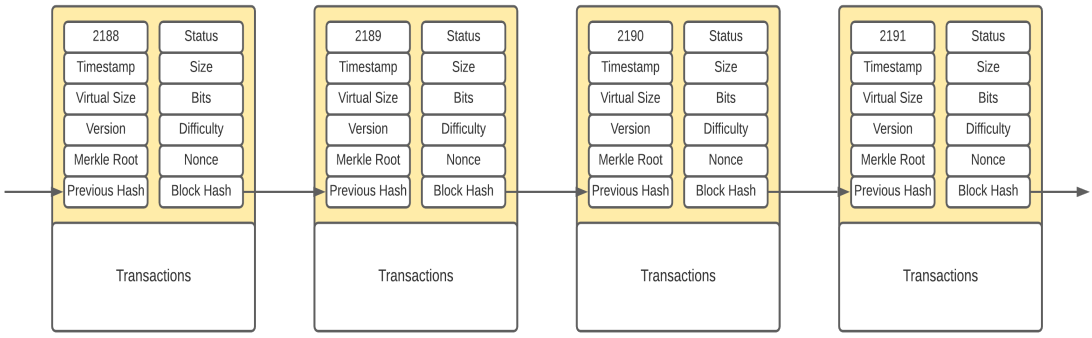

Figure 1.2: Blockchain

1.1.3 Types of Blockchain

Private and public blockchains are the two main styles of blockchains. There are, however, several variants, such as Consortium and Hybrid blockchains.

1. **Public Blockchain:**A public blockchain is a permissionless, non-restrictive distributed ledger scheme. Anyone with an internet connection will sign up with a blockchain platform to become a registered node and join the network. A public blockchain node or user is allowed to access current and historical data, validate transactions, and perform proof-of-work for an incoming block.The most basic use of shared blockchains is for cryptocurrency mining and exchange. As a result, Bitcoin and Litecoin blockchains are the most widely used public blockchains. If users strictly obey security rules and methods, public blockchains are largely stable. However, it is only dangerous where the members do not adhere to the security protocols.

2. **Private Blockchain:**A private blockchain is a permissioned or restricted blockchain that can only be used in a secure network. Private blockchains are typically used by a company or corporation where only a few people are allowed to participate in a blockchain network. The governing organisation determines the standard of compliance, authorizations, permits, and usability.As a result, private blockchains are similar to public blockchains in terms of functionality, but they have a smaller and more restricted network. Voting, supply chain management, digital identities, wealth ownership, and other applications use private blockchain networks.

3. **Permissiond Blockchain:** A consortium or permissioned blockchain is a semi-decentralized type in which a blockchain network is managed by several organizations. This is in contrast to a proprietary blockchain, which is controlled by a single entity. In this sort of blockchain, more than one entity may serve as a server, exchanging information or mining. Banks and government agencies also use consortium blockchains.

4. **Hybrid Blockchain:**A Hybrid blockchain combines the advantages of both proprietary and public blockchains. It combines the benefits of both private

and public blockchains, allowing for both private and public permission-based systems. Users will monitor who has access to which data held in the blockchain with a hybrid network like this.Users can conveniently join a private blockchain or several public blockchains thanks to the hybrid blockchain system's flexibility. A transaction in a hybrid blockchain's private network is normally checked inside the network. Users should, however, publish it on the public blockchain to be checked. The hashing power of public blockchains is increased, and more nodes are involved in the verification process.This improves the blockchain network's stability and accountability.

1.1.4 Properties of Public Blockchain

- **Decentralization:** Peer to Peer (P2P) is a decentralized network communications model that consists of a group of devices (nodes) that collectively store and exchange files, with each node acting as a single peer. P2P communication takes place in this network without the use of a central administration or server, which ensures that all nodes have the same control and perform the same tasks.
- **Distributed Ledgers:** A distributed ledger is a type of database that is shared, replicated, and synchronized by decentralized network participants. A copy of blockchain works as a ledger.
- **Immutability:** The potential of a blockchain ledger to remain unchanged, for a blockchain to remain indelible, is known as immutability. To put it another way, data in the blockchain cannot be changed. Each block generates an alphanumeric string, which is used to generate the hash value. Any block includes a hash or digital signature for both itself and the previous block.This feature of blockchain technology means that no can change the information stored in the block.
- **Anonymity:**Each user can interact with the blockchain network with a generated address which is anonymous.
- **Auditability:** The property is that blockchain are automatically timestamped.

This implies that it assists in a decentralized manner. So, that aids in determining what data has changed and how data has changed when a record has been modified. Who kept it up to date on this sort of thing? These characteristics make blockchain so intriguing.

1.1.5 Consensus Mechanism:

1.1.5.1 Why consensus?

Since a blockchain is a decentralized peer-to-peer system with no central authority figure, it requires a way to monitor the system's official current state. This gives rise to two problems: How is any decision made? How does anything get done?

1.1.5.2 What is Consensus?

The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, cooperation, equal rights to every node, and mandatory participation of each node in the consensus process. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.

1.1.5.3 Consensus Algorithm

A consensus algorithm is a method by which all peers in a Blockchain network reach a consensus on the current state of the shared blockchain. Even if certain agents fail, it must ensure that all agents in the scheme rely on a common point of fact. To put it more simply, the system needs to be fault-tolerant.

1.1.5.4 Consensus Algorithm Properties

1. **Fault Tolerance:** A byzantine fault is unique to a distributed system that is attempting to reach a consensus between its nodes. If a node/component in a distributed system is producing: erroneous data, misleading information, or even no information at all, it can be considered a byzantine fault. A more conventional BFT algorithm necessitates that more than two-thirds of the system's nodes be "non-byzantine," or behaving in a desirable manner.

However, not all consensus algorithms need this; for example, Bitcoin and Ethereum consensus algorithms require that 50% of nodes be non-byzantine in order to maintain security.

2. **Termination:** At some stage, the right method must settle on a value.

3. **Integrity:**Any right method would determine whether all the correct processes recommended the same meaning.

4. **Acceptance:**Any right procedure must agree on a common value.

1.1.6 Issues & Challenges of Public Blockchain

1. **Increasing Data Storage:** The data on blockchain ledgers is permanent, which means it can't be changed, erased, or relocated. The peer-to-peer design of blockchain networks becomes a concern as a result of this. If each participant keeps a complete working copy of the blockchain, all data added to it must be copied to the hard drives of all network participants. The Bitcoin blockchain's size is more than 320 GB now. Each node on the network must have more than 320 GB to synchronize with the bitcoin network and hold upcoming blocks. This increasing size of the blockchain makes the system more expensive to handle.

2. **Scalability:** The blockchain industry's ability to handle a vast number of transactions at once remains a challenge. To perform a single transaction, blockchain technology uses many complex algorithms. Where VISA can handle on average around 1,700 transactions per second (tps), Bitcoin handle 3.15 to 7 transactions per second(tps) [1] [2] and Ethereum, can only process about 17 transactions per second(tps) [3].

3. **Privacy:** Though pseudonymous user addresses are used, however users transact with the same address regularly, it is still possible to connect addresses to actual identities.

4. **Irreversibility:** Data or transactions can't be reversed if they've been appended and approved by a network. However, a blockchain may only

guarantee validity, not reliability and accuracy. Fake information will end up on a blockchain if it is provided correctly.

1.2 Framework/Design Overview

There are two parts. One is a new blockchain scheme and another is its consensus algorithm. In the proposed scheme, there are 'n' mini-shard chains and each block of a mini-shard chain contains the previous block hash and the previous chain's block hash. For example, five-number block of the second mini-shard chain will hold four number block hash and four number block of the first mini-shard chain's hash. Thus this scheme will build an immutable blockchain scheme.

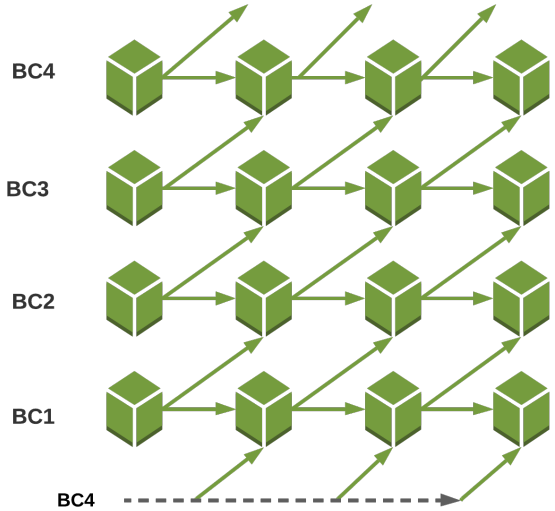

Figure 1.3: An Overview of the Proposed Scheme

For the Proposed scheme, A new consensus algorithm is required which goes with the structure. To achieve the goal, I develop a consensus algorithm named Proof of Duty(PoD). The PoD is the algorithm where each node has shown their dedication through their duty on the network. Each node has a duty level. Using this duty level a forger's committee and a validator's committee get selected. For a round, this two committee works together to add malicious free transaction in the block hence the chain. They get rewards for their work at the end. Hare each round is divided into a number of slots. A slot is dedicated to adding one block.

1.3 Difficulties

- Satoshi Nakamoto launched blockchain technology in the form of Bitcoin in 2008. It is still new to people. As a result, there are insufficient educational resources to understand and learn about it.
- It has not been widely adopted in the industry due to a lack of experience and skills. This makes experimenting and testing a challenging task.
- As blockchain is implemented in a decentralized manner, it is difficult to experiment with a new blockchain scheme and consensus algorithm.

1.4 Applications

Public Blockchain mainly is used for cryptocurrency. Cryptocurrency is used for a wide range of applications. Such as:

- **Wealth Management:** One of the most exciting applications of cryptocurrency is wealth management. That's why companies like SwissBorg, which has developed its own tokens for investment solutions, are providing investors with exciting new ways to handle their wealth without limitations.
- **De-corrupting charities:** Additionally, cryptocurrency can be used to protect charity organizations against corruption. Blockchain will remove multiple issues that plague charities, such as fund leaks, due to its potential to hold organizations accountable. That is why the World Food Programme (WFP) is using blockchain to deliver cash aid to the needy in a safe manner.
- **Raising funds:**Cryptocurrencies are also being used by many startups to finance their inventions, services, and products. Rather than relying on conventional VC financing or crowdfunding platforms like IndieGoGo or Kickstarter, entrepreneurs are turning to cryptocurrencies as a means of raising funds. It's revolutionizing the whole fund-raising process because it's too simple to track and obtain funds this way.

1.5 Motivation

The motivation of proposing a new blockchain scheme for cryptocurrency public blockchain is given below:

- With the advancement of blockchain technology, people now understand the importance of blockchain. As a result, users and transactions on the blockchain are growing exponentially. But the traditional scheme is not able to scale with the growing use.
- Consensus Algorithm is the main factor to add a block hence make scalable a blockchain platform. But the conventional system of consensus of public blockchain has some limitations. As a result, It makes the system less secure and power-consuming.
- Blockchain is a distributed ledger that means each node in the network holds a copy of the ledger. But the size of the blockchain is not constant. It's increasing day by day. Hence, storing the whole ledger is getting difficult for a node.

1.6 Contribution of the thesis

Thesis or research activity is done to accomplish a certain set of objectives, whether they be academic or professional to create a new approach or improve the existing ones or define a new methodology. The primary emphasis of this research was on solving scalability problems and increasing blockchain size problems. The main contribution of this thesis is the following:

- Designed a new blockchain scheme named 'Mini-Shard Chain'
- Proposed its consensus algorithm 'Proof of Duty'
- Evaluated overall performance by giving mathematical and theoretical proof
- Presented a table of comparisons to evaluate the proposed work's performance

1.7 Thesis Organization

The rest of the report is sequenced as follows: In the next chapter, Literature reviews of existing blockchain schemes and their consensus algorithm. In chapter 3, The approach used to accomplish the work's goal is well explained and elaborated. In the chapter, I describe the new blockchain scheme and its consensus algorithm. In chapter 4, I describe the analysis of the performance measure for the proposed method and implementation. In chapter 5, I concluded the whole work and briefly summarized the impact of our work on future works that can be done.

1.8 Conclusion

A summary of the project is given in this chapter. The chapter introduced related concepts to the reader. Also, the challenge faced and the application of this work are briefly discussed. The importance of the work is mentioned in the motivation section and contribution of the work is also provided. The works of previous researchers in this field of study will be discussed in the next section.

Chapter 2

Literature Review

2.1 Introduction

An overview and the significance of the work are presented in the previous chapter. The work's contribution and implementation are both mentioned. In the past eight or nine years, a few types of research have been conducted to design an efficient lightweight scalable blockchain. There are a lot of consensus algorithms implemented in different types of blockchain. But consensus algorithms for cryptocurrency which is mainly built on public blockchain are few. In this chapter, The relevance of the researchers' analysis is assessed and the framework is illustrated. The core aspects of the studies, as well as the techniques used to obtain the results, are also discussed. The outcomes of scholarly publications are examined in order to provide a better understanding of the present situation. The literature review is divided into two parts. The first part represents the different cryptocurrency blockchain schemes and the second part represents the consensus algorithms.

2.2 Related Blockchain Scheme

In [4] Satoshi Nakamoto was first invented cryptocurrency is called Bitcoin. The blockchain is a shared public ledger that underpins the whole Bitcoin network. The blockchain contains all authenticated transactions. It enables Bitcoin wallets to measure their spendable balance, allowing new transactions to be checked and ensured to be held by the spender. Cryptography is used to ensure the blockchain's legitimacy and chronological order. A transaction is a value transfer between Bitcoin wallets that are recorded in the blockchain. Bitcoin wallets store

a private key, also known as a seed, which is used to sign transactions to provide cryptographic proof that they came from the wallet's user. Bitcoin uses proof of work(PoW) as a consensus algorithm. To reach consensus in a decentralized way to deter bad actors from overtaking the network, PoW allows nodes on a network to have proof that they have expended computational power. Though Bitcoin is the most valuable cryptocurrency, it has a lot of drawbacks. It's not scalable. Its mining process is power-consuming. A huge loss could be the result of a 51% attack.

In [5] Vitalik Buterin introduced Ethereum in 2013. It is the first version of Ethereum. With several significant variations, Ethereum draws on Bitcoin's innovation. Ethereum is a decentralized, open-source, blockchain-based computing framework that operates using its own cryptocurrency, ether. It allows Smart Contracts and Distributed Applications (DApps) to be designed and run without the risk of downtime, theft, regulation, or third-party intervention. Its drawbacks are similar to Bitcoin.

Ethereum 2.0 (Eth2) is an enhancement to Ethereum's scalability, stability, and long-term sustainability [6]. Despite the fact that they are all being worked on in parallel, they have certain requirements that dictate when they will be deployed. Eth2 brings the concept of beacon chain and shard chain. Sharding is the method of horizontally splitting a database to increase the scalability and capacity of Ethereum. Shard chains distribute the load of the network through 64 new chains. Validators just need to store or run data for the shard they're validating, not the entire network. They make running a node simpler by lowering the hardware specifications. The extended network of shards and stakers would be controlled or coordinated by the Beacon Chain. The Beacon Chain will introduce proof-of-stake to Ethereum. The Beacon Chain introduces proof-of-stake to Ethereum. The advantages of ethereum 2.0 over the previous ethereum protocol are many. Ethereum 2.0 is more scalable and secure. It uses proof of stack to reach a consensus which is not power-consuming unlike proof of work mining. The main disadvantages of ethereum 2.0 are the Single-Shard Takeover Attack was to build a malicious shard, the attacker just needs to gain control of the plurality of collators in a single shard and nothing at stake problem[7]. Moreover, eth2 maintains an

extra beacon chain that stores all of the logic for holding shards safe and in sync.

In [8] J.D.Bruce has introduced Cryptonite. Cryptonite is a mini-blockchain scheme that is built on a conventional blockchain scheme. Cryptonite is a peer-to-peer (P2P) cryptocurrency that allows the network to forget about old transactions. We call this portion of the chain the mini-blockchain because nodes only need the most recent portion of the blockchain in order to sync with the network. The account tree, a directory that contains the balance of all non-empty addresses, is used to prevent the loss of coin ownership records. As nodes discard old blocks, only the transactions are discarded, not the block headers. The proof chain is a chain of block headers. The proof chain secures the mini blockchain and the account tree is secured by the mini blockchain. The main advantage of it is the storage optimization characteristic and the account tree where nodes on the network don't require previous transactions to calculate the balance of any given address.

2.3 Related Public Blockchain Consensus Algorithms

This segment will go through some well-known consensus algorithms, how they perform, and their benefits and drawbacks.

2.3.1 Proof of Work(PoW)

PoW [4] [9] [10] is an algorithm for the Bitcoin blockchain. In the Bitcoin scheme, the consensus is achieved by a time-consuming mechanism that necessitates the use of high-performance computing capabilities such as Application Specific Integrated Circuits (ASICs) or Graphics Processing Units (GPUs). In this algorithm, miners try to solve a mathematical problem to get the desired result. According to the bitcoin whitepaper [4], miners change the nonce portion of the corresponding block and search for a hash that starts with a number of zeros. How many zeros will have to be in front of the hash will be determined by difficulty level.

2.3.1.1 Advantages of PoW

- Defense from DOS attacks
- The holders of huge amounts of money are not in charge of making decisions for the entire work.
- The cost of destroying the system is huge.

2.3.1.2 Disadvantages of PoW

- A high amount of power and energy is required.
- More powerful ASICs have a better chance of mining.
- 51% attack

2.3.2 Proof of Stake(PoS)

Ethereum 2.0 introduced a proof of stake consensus model [9] [10] [6], which builds on the principles behind proof of work. Proof of stake models is based on how much cryptocurrency a node, or validator, put "at stake." The more bitcoin a validator stakes, the more mining power they provide. The PoS algorithms choose a miner for block formation at random, and no miner can predict their turn ahead of time. If Miners create a block, which is then linked to the blockchain, the miner will be paid, but if it fails to add a block to the blockchain, the miner will be punished.

2.3.2.1 Advantages of PoS

- Do not require the computational power
- Prevent 51% attack

2.3.2.2 Disadvantages of PoS

- Nothing-at-stake problem [11]
- Result in a less decentralized network [12]

2.3.3 Stellar Consensus Protocol (SCP)

The Stellar Consensus Protocol (SCP) [13] allows individuals to reach an agreement without having to rely on a closed mechanism to keep track of financial transactions. The Stellar Consensus protocol algorithm [13] makes use of the quorums and quorum slices concepts. A quorum is a necessary number of nodes to reach an agreement. A quorum slice is a portion of a quorum that may persuade a certain node to agree. Individual nodes can appear in several parts of the quorum. Stellar introduced quorum slices to allow each individual node to select a group of nodes in its slice to allow open participation. Quorums must cross to achieve global consensus across networks. Specific node decisions are aggregated to form the global consensus.

2.3.3.1 Advantages of SCP

- Flexible trust
- Low latency
- Energy Saving

2.3.3.2 Disadvantages of SCP

- The entire system could fail in sequence if only the two nodes operated by the Stellar foundation are deleted [14].
- The system is highly centralized in a few specific nodes

2.3.4 Ripple Protocol Algorithm

Each server maintains a unique node list, which is a set of other servers that s queries when determining consensus. Every server first makes public all relevant transactions it has seen before the start of the consensus round that has not yet been added in the form of a list known as the "candidate set." The candidate sets of all servers on the UNL are then combined, and each server votes on the veracity of all transactions. Transactions of more than a certain number of "yes" votes move to the next round. A minimum of 80% of a server's UNL agreeing on

a transaction is needed in the final round of agreement. The transactions that satisfy this criterion are recorded in the ledger, which is then closed and becoming the new last-closed ledger[15] [10].

2.3.4.1 Advantages of Ripple

- System can reliably detect if the network can't reach a consensus.
- An attack or disruption is determined by signed cryptographic proof showing who did it and what they did.

2.3.4.2 Disadvantages of Ripple

- The process of reaching a consensus is highly centralized.
- If UNL is broken, you will fail in a variety of ways, with the degree of the failure increasing as the UNL becomes more broken.

2.3.5 Tendermint

Tindermint [16] [10] was created to solve the speed, scalability, and environmental concerns that exist in the PoW. It uses the PBT algorithm. The tendermint blockchain will handle approximately 33% of byzantine actors in the network. The validator is responsible for verifying transactions and adding new blocks to the blockchain. By broadcasting cryptographic signatures that serve as votes,validators participate in the consensus protocol. To become a validator in the tendermint network, a person must first keep a certain amount of tokens for a period of time and then lock it as voting power. The chance of losing these tokens is present if the validator is not working according to the rules defined by the protocol. The algorithm works as follows: The Propose stage is the first. The appointed proposer for that round broadcasts a proposal to its peers through gossip at the start of the Propose step. The next step is the prevote step. During the Prevote step, all nodes gossip all prevotes for the round to their neighboring peers. The validator signs and broadcasts a pre-commit for a specific suitable block if it has obtained more than 2/3 of the votes for that block. Each node

decides at the end of the pre-commit process. The node enters the Commit step if it has obtained more than 2/3 of the precommits for a given block.

2.3.5.1 Advantages of Tendermint

- PBFT consensus
- Power saving
- Tendermint achieves low latency with protection by using a limited jury of trusted validators [17]

2.3.5.2 Disadvantages of Tendermint

- Since it has a higher number of messages than the other protocols, the composition of a jury cannot be too big. Tendermint is also a good protocol for Data exchange's side chains, but not for its main chain. [17]

2.4 Conclusion

In the chapter, I have discussed those papers which helped me to develop a new robust scheme and an efficient algorithm. The brilliant approaches of blockchain and its consensus, their pros, cons, working process, etc have been reviewed in the section. The proposed blockchain scheme and consensus algorithm will be discussed in the next chapter

Chapter 3

Methodology

3.1 Introduction

There are a few kinds of research that are trying to solve both the scalability and increasing blockchain size issues. The beacon chain and shard chain concept of ethereum 2.0 [6] makes their blockchain system scalable. But the problem arises on the point of storage optimization. Each node of ethereum 2.0 keeps track of only the shard chain the node is validating [18]. Though ethereum 2.0 reduces the pressure of storing the entire blockchain to storing only the shard chain, with the increasing popularity of ethereum , after a few years the validator nodes of each shard chain will face the same issue. On the other hand, the mini-blockchain scheme [8] can optimize the storage of each node on the network but it is not scalable. In this chapter, I will describe a new blockchain scheme and an improved consensus algorithm to make a robust solution that will be scalable and optimize storage. The methodology will be divided into two parts. The first one is the proposed blockchain scheme and the second one is the consensus algorithm.

3.2 Proposed Blockchain Scheme

The proposed scheme consists of 'n' blockchain instead of one blockchain where 'n' is an integer number. Each chain of the proposed scheme can be called a mini-shard chain. A fixed number of nodes keeps a copy of a mini-shard chain. A node of a mini shard chain doesn't require keeping the copy of another mini-shard chain. The number of n depends on two factors. They are:

1. **The Number of Transactions per Second:** More blockchain can handle more transactions per second (tps).

2. **The Number of Nodes:** Decentralization secures the blockchain. A blockchain can be made more secure by increasing the number of nodes.

3.2.1 Block Elements of Mini-Shard Chain

The block of the proposed scheme contains some extra data than the traditional blockchain's block. They are:

1. **PCLB Hash and Previous Hash:** A block of n^{th} chain (Height m) holds hash of $(m\text{-}1)^{th}$ block and hash of $(m\text{-}1)^{th}$ block $(n\text{-}1)^{th}$ chain. Example: 337^{th} block of 2nd chain will hold hash of 336^{th} block and hash of 336 block of 1^{st} chain. Thus, A block of 1^{st} chain (Height m) holds hash of $(m\text{-}1)^{th}$ block and hash of $(m\text{-}1)^{th}$ block (n^{th} chain)
2. **Validation Merkle Root:** It is a root hash of all validator signatures. Each signature's hash is the leaf node of the Merkle tree.
3. **Forger's Signature Hash:** It is the hash of forger's signature
4. **Transactions Merkle Root:** It is the Merkle root hash of all transactions

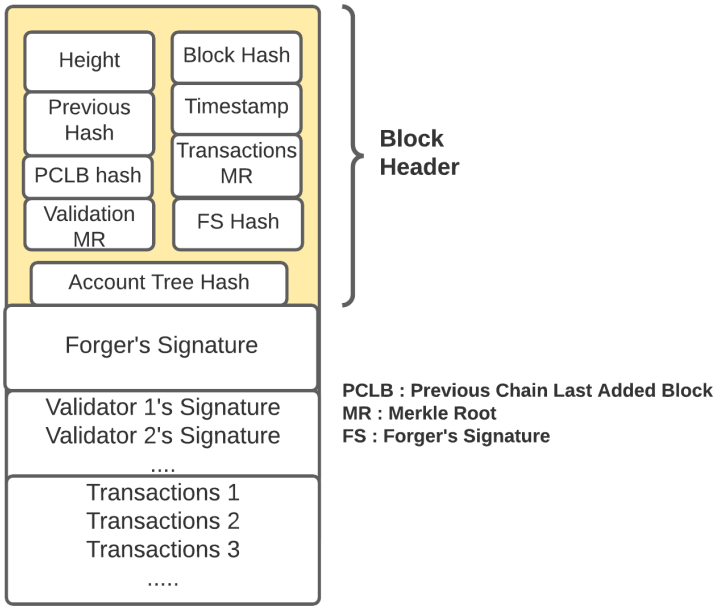

Figure 3.1: A Block of Proposed Scheme

When all we need to know the balance of all non-empty addresses, why should

we log every single transaction and store it forever? The solution belongs to the concept Mini Shard Chain, Proof Chain, Account tree [8]

3.2.2 Mini-shard chain

The mini-shard chain is built on the mini-chain and shard chain concept. With the growing size of the blockchain, sharding is a scalable solution where a blockchain is split into n numbers of shard chains. The use of sharding would minimize network latency and increase the number of transactions per second [6]. On the other side, the mini-chain is the recent portion of the chain. Transactions of old blocks will be forgotten by the network. In summary, we can say that The mini-blockchain is the same as a regular blockchain, with the exception that we don't need to hold a backup of previous blocks [8].

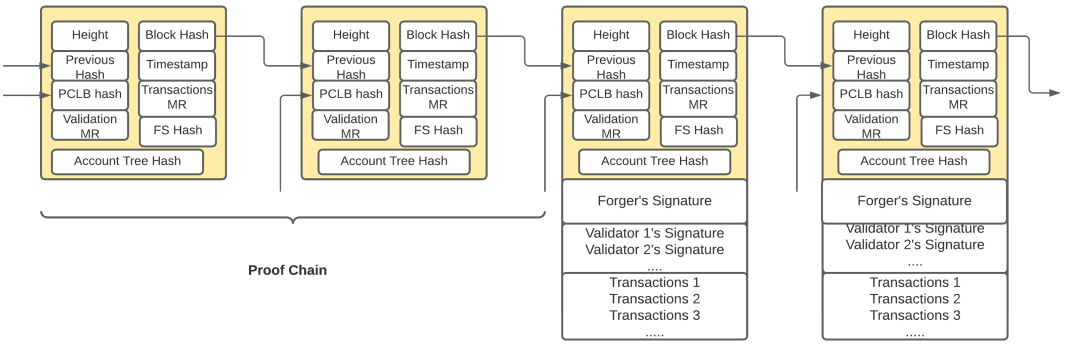

Figure 3.2: A Mini-Shard Chain

3.2.3 Proof Chain

The proof chain is simply a chain of block headers. As nodes discard old blocks, only the transactions are discarded, not the block headers. So, the mini-blockchain is essentially a blockchain that has been pruned with everything but the most current transactions. This ensures that all nodes can continue to use the chain of block headers to validate the best mini-blockchain with the greatest total complexity, and they can measure address balances without relying on old transactions with the help of the account tree.

3.2.4 Account Tree

The account tree can be related to a decentralized "balance sheet." It will include any non-empty address, as well as the balance of all those addresses, as well as a few other fields that allow for withdrawal limits. Instead of applying new data to the account tree when the balance of an address change, what we have to do is correct the numbers in the account tree. Of course, since new non-empty addresses will emerge all the time, this will never have a completely finite number of data to deal with, although it will come as near as possible. It is finite in several ways because the coins would have little divisibility, and we can't allow the global population of Internet users to keep expanding indefinitely. The account tree can be applied in a variety of ways, but the data structure must meet the following criteria:

- A deterministic hash (master hash/ledger fingerprint) should be capable of effectively summarizing all results.
- It must Support for four operations: add an account, change account, delete account, and lookup account is effective.
- The account tree master hash should be updated easily for each change.
- It should be possible to verify the correctness of a subset of the accounts without having to import the whole structure.

3.2.5 Network

1. Each node on the network doesn't require to hold all mini-shard chain
2. A particular set of nodes will hold the same copy of the mini shard chain. They keep track of only the shard chain the node is validating.
3. Each node on the entire holds the same account tree. It will be ensured by the account tree hash

In 3.3, we can see the proposed blockchain scheme with four MSC where each block holds its previous block hash and the previous chain's block hash. In 3.4,

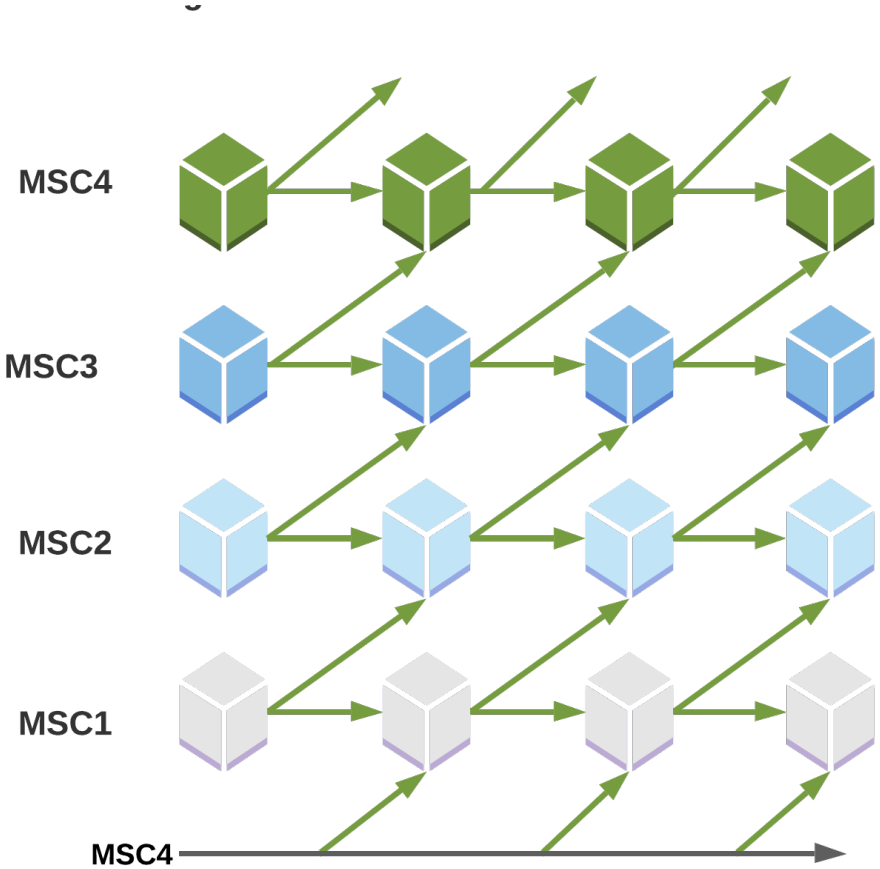

Figure 3.3: Proposed Scheme When n=4

each mini-shard chain maintains by its own nodes but all the nodes in the network maintain a common account tree and that account tree hash.

3.3 Consensus

3.3.1 Consensus Committee

Consensus Committee consists of two sub-committees. The two subcommittees are

1. Forgers
2. Validators

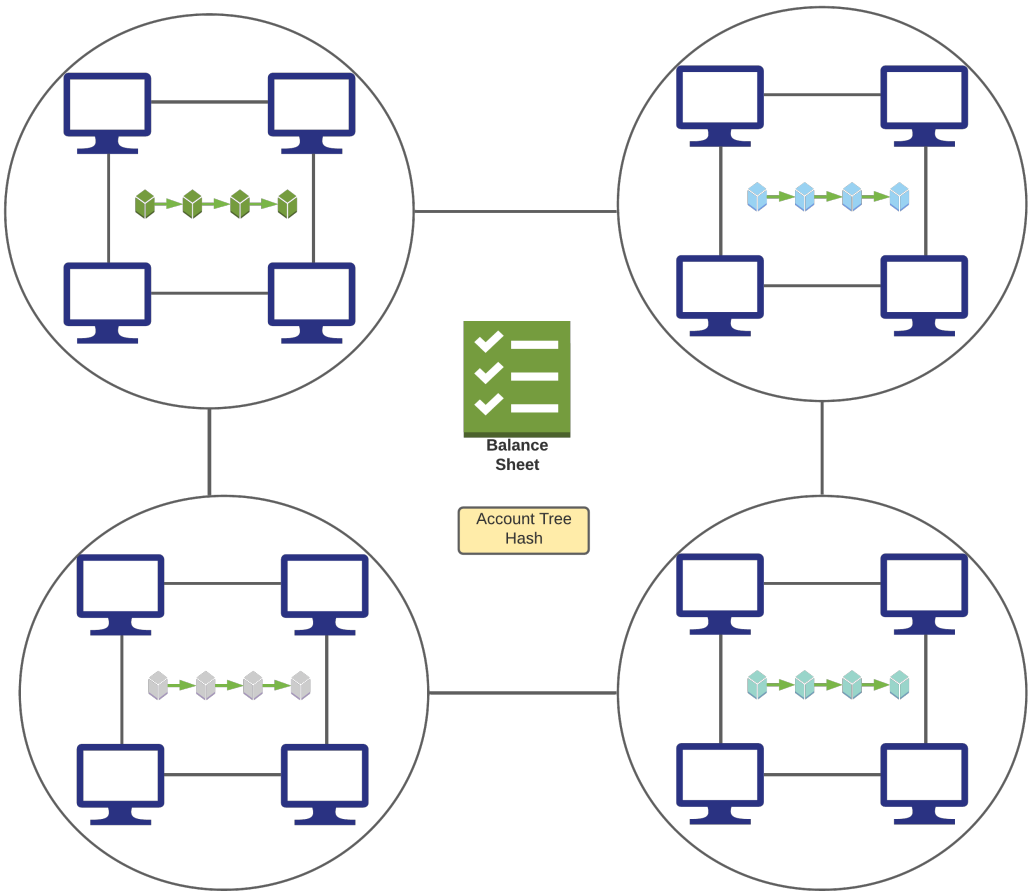

Figure 3.4: Network Overview When n=4

3.3.2 Feature of nodes

- **Network activity ratio:** Internet traffic determines the network activity ratio of a node. The flow of data in certain network connections of the Internet's constituent networks is known as traffic.
- **Validated block ratio:** The number of blocks added to the chain which was validated by a node is the total number validated block of that node. Validated block ratio is the ratio of the number of validated block of a node to the current size of the blockchain
- **Duty Level:** Each node have a duty level which will be determined by staked coin, network activity ratio and validated block ratio.

3.3.3 Forgers Selection Process

1. To enter into the forger's committee, a node must lock a predetermined number of coins into the stake.
2. The algorithm will set a level on each round. All the nodes above the level will be selected for preselection
3. A set of nodes will be selected randomly from the preselected set will work as Forgers

3.3.4 Validators Selection Process

1. To enter into the Validator's committee, a node must lock a few coins into the stake. But the value of the staked coin is less than the value set for the forger.
2. Those nodes have the highest network activity ratio and validated block ratio they will be preselected for validation
3. A set of nodes will be selected randomly from the preselected set will work as validators

3.3.5 Round

A consensus committee will be selected for a round. Each round is divided into a certain number of slots. Here I consider a round of 5 minutes where each slot 10second. So a total of 30 slots is fixed for a round. Each slot will add a new block by the committee. A node can withdraw its coin after completing a round.

3.3.6 Proof of Duty(PoD)

1. Before going to the consensus process, each forger and validators ensure they have the same account tree hash.
2. A node will be selected randomly from the forger committee for each slot of a round.
3. That forger node create a block and send it to the validators pool

4. The validator committee checks all transactions of the block. If a transaction gets 30% downvote for being malicious transactions, it will be discarded from the block.

5. Each validator validates the block by giving a signature, It may be called a vote.

6. If the block gets 2/3 votes of validators, it will be added to the blockchain.

7. after adding the block, each node will update its account tree

8. The reward for the forger is the product of reward value and transaction acceptance ratio for that block. Transaction acceptance ratio is the ratio of the transaction accepted to transaction submitted for that block. For example: The transaction submitted by the forgers is 2000 where 200 malicious transactions are discarded by the validators. As a result, the number of transaction accepted is 1800. The transaction acceptance ratio for the forger is 0.9. If the reward value is 6, the reward of the forger's is 5.4.

9. The transaction fees and the remaining part of reward will be distributed to the validators.

10. For their malicious actions, each node on the committee will receive a punishment. The punishment will decrease the duty level of that node hence lose their staked coin.

3.4 Conclusion

In the chapter, A new scheme of blockchain and its consensus algorithm, Proof of Duty(PoD) has been introduced. I tried to explain the structure of the scheme, how they operate in the network and most importantly how they come to an agreement. In the next chapter, I will show the proposed scheme and PoD give an efficient solution than the existing system.

Chapter 4

Results and Discussions

4.1 Introduction

A new blockchain scheme and its consensus algorithm have been proposed in the previous chapter. The structure of the proposed scheme, its network structure and its consensus mechanism named proof of duty also explained in that chapter.

In this chapter, I will prove the proposed scheme is scalable and optimize the storage requirement of the node. A comparison between public blockchain consensus algorithms and proof of duty will be presented also.

4.2 Performance Evaluation of Proposed Scheme

4.2.1 Security Enhancement

4.2.1.1 More Immutable Chain

The conventional block arrangement in a blockchain is immutable. Immutability ensures the ability of a blockchain ledger to remain unaltered or unchanged. Each block contains the previous block hash. If anyone wants to change the data of a block, it has to change the rest of the block of the chain.

In the proposed scheme, A block holds not only the previous block hash but also the block hash of its prior shard chain. So if anyone wants to change the data of the block, it has to change the rest of the block of the shard chain and the descendant chain. So it is more immutable than a conventional blockchain scheme.

In the figure 4.1, We can see a change in the second number block is the reason

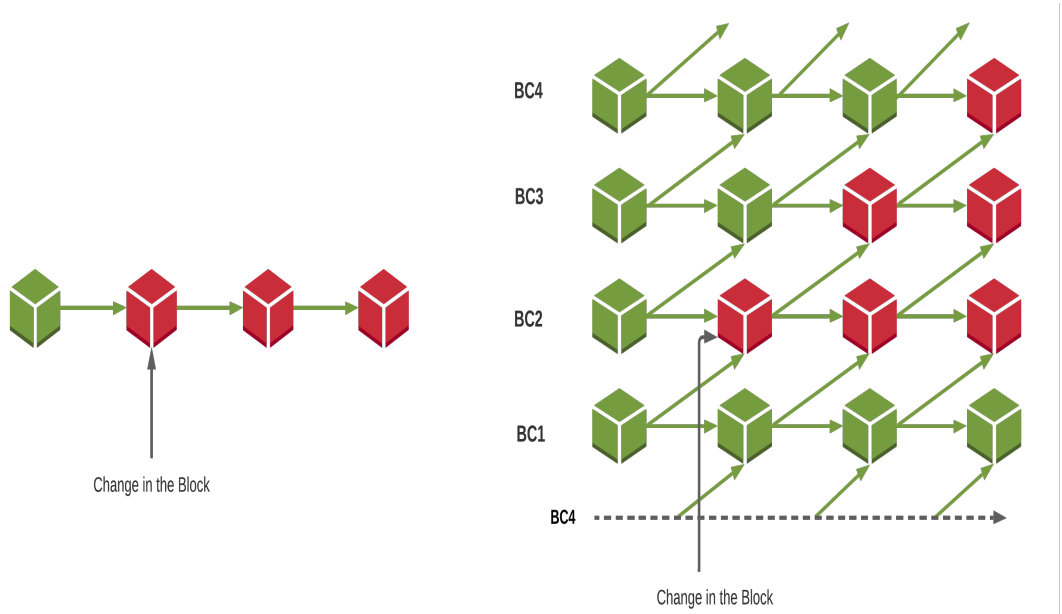

Fig: Traditional Blockchain Scheme

Fig: Proposed Blockchain Scheme with Four Mini-shard Chain

Figure 4.1: Traditional Blockchain Scheme vs Proposed Blockchain Scheme

for changing the remaining 3 blocks in the traditional scheme where a change in the second no block of the second blockchain is the reason for changing the remaining 6 blocks. So the proposed Scheme is more secure.

4.2.2 Optimizing Storage Requirement

A full node of a conventional blockchain system holds all data of the entire blockchain system [4]. A node proposed scheme doesn't require storing the entire blockchain data. It only maintains a mini-shard chain of the entire blockchain system. Moreover, a mini-shard chain holder doesn't store the entire shard chain where old block's transactions are forgotten by the network.

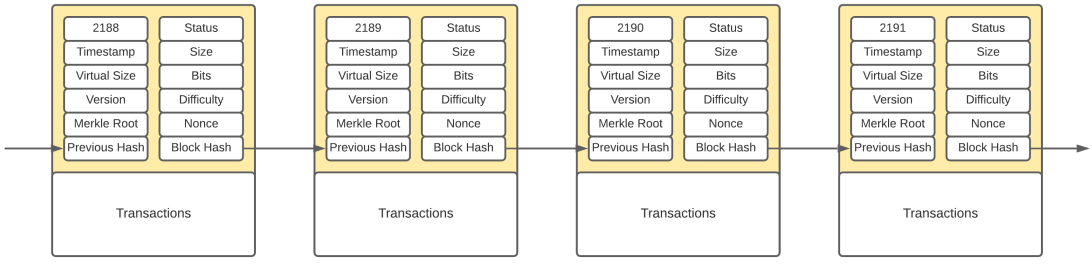

Figure 4.2: The Structure of Traditional Blockchain

Let's assume,

Average Transactions per Block= p

Average Transaction Size = s_1

Height of the Blockchain= m

Block Header Size=s_2

In Traditional Blockchain Scheme, Blockchain Size = TBS

$$TBS = \sum_{i=1}^{m} ps_1 + ms_2$$

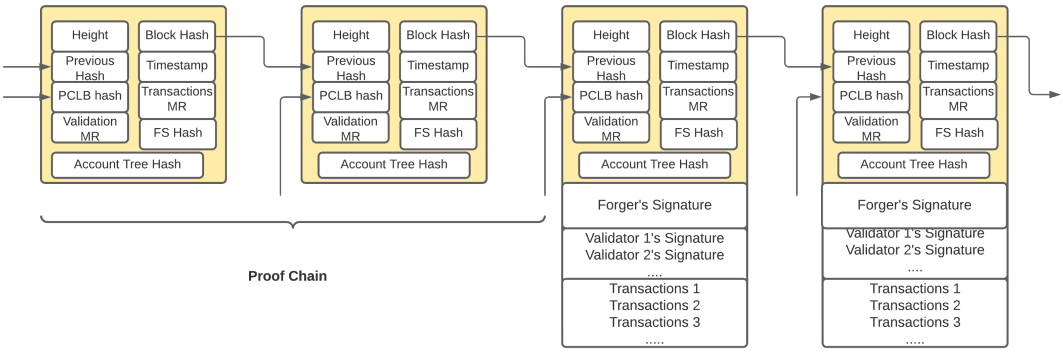

Figure 4.3: The Structure of Mini-Shard chain of the Proposed Scheme

Again, In the Proposed Blockchain Scheme,

Total Mini-Shard Chain=n

Mini-Shard Chain Size= MSCS

Proof Chain Height= q, where q<m

$$\begin{aligned} MSCS &= \frac{\sum_{i=1}^{m} ps_1 - \sum_{i=1}^{q} ps_1 + ms_2}{n} \\ &= \frac{\sum_{i=q+1}^{m} ps_1 + ms_2}{n} \\ &= \frac{TBS + \sum_{i=1}^{q} ps_1}{n} \end{aligned} \tag{4.1}$$

So,

$$TBS = nMSCS + \sum_{i=1}^{q} ps_1$$

As TBS>MSCS , we can say a node of a traditional blockchain scheme is required more storage than a node of the proposed blockchain scheme.

4.2.3 Scalability

In Blockchain, Scalability refers to securing transactions per second (tps). The scalability of a blockchain-based application depends on two factors. one is the time required to reach a consensus and blockchain structure.

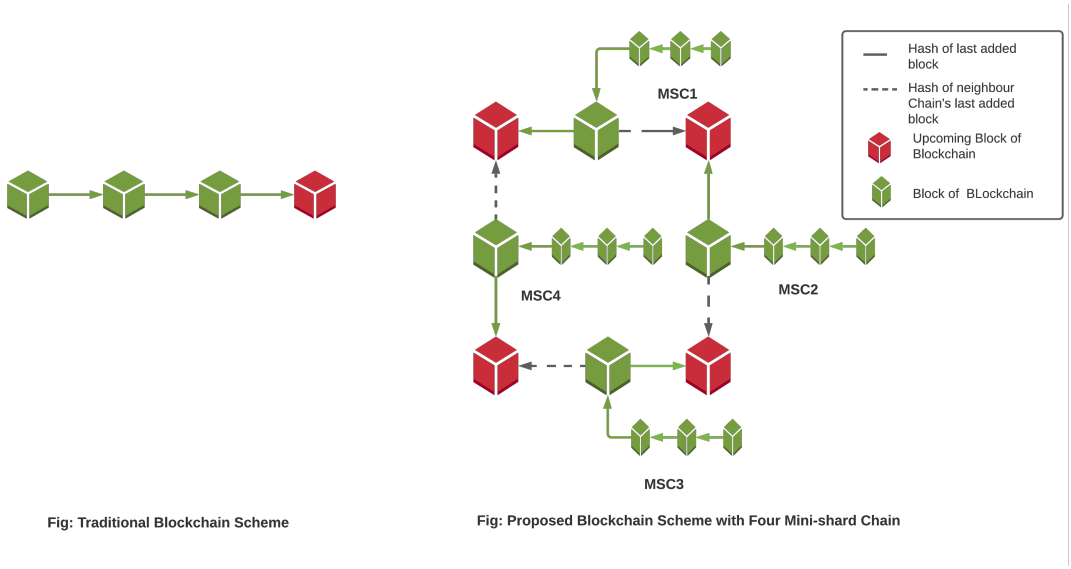

Figure 4.4: Scalability Comparison

4.2.3.1 Time Required to Reach a Consensus

According to this [19], three criteria of a consensus algorithm determine whether it would be scalable or not?

- Is the blockchain using the Bitcoin PoW consensus method? If that's the case, the PoW isn't scalable.
- If a blockchain system is using BFT type consensus algorithm, has the algorithm a smart trick to reduce message complexity? If no, it's not scalable.
- Is it necessary for each validating/mining node to be informed of every message? The nodes participating in consensus are referred to as "nodes." If yes, the blockchain is not scale-out.

The proposed consensus algorithm, PoD is neither applying PoW nor build on a Pow-based algorithm. It meets the first condition. The PoD algorithm is developed on the PBFT algorithm where a set of validators give votes using signature. They gossip through messaging. PoD doesn't allow all nodes to participate in consensus. It selects a particular set of nodes randomly for a round and they generate blocks. As a result, it fulfills the third point and the second point partially. So, It confirms that the PoD algorithm makes the system scalable.

4.2.3.2 Blockchain Structure

When a regular blockchain adds a block, here the proposed scheme adds 'n' blocks at a particular time. Here, 'n' is the number of mini-shard chains.
In this case, We assuming both schemes run on the same consensus algorithm apart from their own algorithm. It ensures both schemes add a block at the same time.

Let's assume,
Average Transactions per Block= p
Average Time Required Adding a Block then=t
Scalability of Regular Blockchain Scheme = TB
Scalability of Proposed Blockchain Scheme = MSC

$$TB = \frac{p}{t}(tps)$$

$$MSC = n\frac{p}{t}(tps)$$

It can be said proposed scheme n time scalable than orthodox scheme. If n=4, The proposed scheme handles transactions four times faster than the normal blockchain scheme.

4.3 Comparisons among Blockchain's Schemes

The following table compares various blockchain schemes with properties:

Property	Bitcoin	Ethereum 2.0	Mini-Blockchain	Mini-Shard Chain
Concept	Use regular blockchain	Use beacon chain and 64 shard chains	Use regular blockchain	Use 'n' shard chains
Scalable	No	Yes	No	Yes
Optimize Storage	No	Partial	Yes	Yes
Necessity of extra chain	No	Yes	No	No

4.4 Performance Evaluation of PoD

An article titled 'A Study on Public Blockchain Consensus Algorithms: A Systematic Literature Review' [10] depicts unfair aspects of the public blockchain consensus algorithm. In this section, I will describe how does PoD solve these issues?

- **Unfair Transaction Selection:** Transaction fees prioritize a transaction. More transaction fees increase the possibility of adding the transactions earlier by a miner. Hence the low fees make a transaction unconfirmed day by day.

  PoD solves the problem. The reason behind the solution is a forger creates a block and sends it to the validators. after adding a block the validators get the transaction fees, not the forger. forger only gets the reward. So there is no incentive to choose a high fee transaction for a forger.

- **Energy and computation expenditure :** In bitcoin, the PoW difficulty level continues to rise. As a result, more power and dedicated hardware (such as an ASIC) are needed to overcome the hash value, which increases the costs of locating the hash value by a certain number of zeros in front.

  In PoD, no dedicated hardware is required because this is not necessary to find a desired hash to mine a block. A small amount of computation is needed to detect malicious transactions in the block. So PoD is a power-saving algorithm.

- **Uselessness of Computation:** To find a specific hash value, all miner in bitcoin use their computational power. If one of them is succeeded, the hard work of other miners becomes worthless, and their hard work would not be applied anywhere else.

On another side, a specific set of forgers and validators works to add new blocks. And they don't search for a specific hash spending their computational power.

- **Forking :** Forks are possible in consensus algorithms such as PoW, PoC, PoPF, PoL, DPoS, and PoS Casper due to the selfish greed of miners.As a result, the blockchain is split up into two parts.

  In the proposed consensus algorithm, forgers and validators are preselected by the algorithm and a committee is responsible for inserting blocks into the blockchain in a round. If the committee gets malicious and tries to create a forking state, they will lose their staked coin and reward hence decrease the duty level. Another malicious committee can't build another chain to create a forked state.

- **51% attack:** A 51% attack on a blockchain network occurs when a single person or group has ownership over the majority of the hash rate. In this case, the attacker will have enough mining capacity to exclude or change the order of transactions on purpose. This attack causes create double-spending and neglecting specific user's transactions. So, 51% attack is not possible in the proposed consensus, PoD.

- **Unfair:** Because of the cost of using expensive technologies such as ASIC (PoW), TEE (PoL), and holding stake (PoS, PoS Casper, Tindermint, PoSV, PoC, and CloudPoS), it is not feasible to use for the poor people who wish to join the blockchain as a miner.

  But in the PoD, a small amount of coin has to store at stake to work as a validator. Moreover, the network activity ratio, honesty ratio determine the duty level of the node. So poor people can join in the consensus process using its dedication in the network.

- **Nothing-at-stake:** The nothing at stake theory is the assumption that in PoS, every validator will build on every fork when a fork takes place. If validators mine on both (or more) chains, they will collect transaction fees on whichever fork ends up winning.

  In PoD, a slot of a round is fixed to validate only a block that is created by

forgers. So if the validator committee wants to validate another block at the same time, the algorithm only selects a block. Validators will get the transaction fees of that block.

4.5 Comparisons among Public Blockchain's Consensus Algorithms with PoD

Property	**PoW**	**PoS**	**DPoS**	**Tendermint**	**PoD**
Energy Saving	No	Partial	Partial	Yes	Yes
Unfair	Yes	Yes	Yes	Yes	Partial
Scalability	Low	Low	Low	Medium	High
Unfair Transaction Selection	Yes	Yes	Yes	Yes	No
Uselessness of Computation	Yes	No	No	No	No
Forking	Yes	Yes	Yes	Yes	No
51% Attack	Yes	No	No	No	No
Minting dependency on stake	No	Yes	Yes	Yes	Partial
Nothing-at-stake	No	Yes	Yes	No	No
Tolerated Power of Adversary	< 25% Computing Power	<51% Stake	<51% Validators	<20% Faulty nodes of UNL	<33.3% Byzantine voting power

We can observe proof of duty gives an optimized result than other public blockchain consensus algorithm.

4.6 Conclusion

The chapter shows the performance evaluation of the proposed blockchain scheme, performance evaluation of its consensus algorithm, proof of duty(PoD), and a comparison among different public blockchain consensus algorithm. In this section, we can conclude that the given solution of the scalability issue and storage optimizing issue can solve these issues. This is the first solution that solves these both issues in the same place.

Chapter 5

Conclusion

5.1 Conclusion

The Blockchain is a public ledger technology that is used by all kinds of cryptocurrencies. Blockchains are a shared mechanism for tracking digital currency transactions.Simple terms, the Blockchain is a decentralized database that records transactions. It keeps duplicate versions of the same ledger on several machines connected to the same network. This ledger is spread through the network's computers, which aids in the network's tremendous security.

As a result, one of the most exciting development fields for blockchain technologies is cybersecurity. Threats like computer hacking will continue to grow in importance for businesses of all sizes. These threats can be avoided using blockchain technologies. It keeps data safe while encouraging active users to keep an eye on the Blockchain to ensure that any transaction is genuine.

First chapter contains a description of the blockchain technology. The difficulty encountered and the implementation of this work are also briefly explored. In the inspiration portion, the importance of the work is discussed, as well as the contribution of the work. In the next part, we'll look at the work of previous researchers in this area.

I covered those articles in the literature review chapter that assisted me in developing a new rigorous scheme and an effective algorithm. In this segment, we've looked at some of the more innovative blockchain and consensus methods, as well as their benefits, drawbacks, and working method. In the following chapter, the proposed blockchain scheme and consensus algorithm will be discussed.

The third chapter introduces a new blockchain scheme and its consensus algorithm, Proof of Duty (PoD). I attempted to clarify the scheme's composition, how they function in the network, and, most notably, how they reach an agreement.

In the fourth chapter, I have demonstrate how the proposed scheme and PoD have a more effective solution than the current arrangement. The chapter examines the proposed blockchain scheme's results, as well as the consensus algorithm's performance, proof of duty (PoD), and a study of different public blockchain consensus algorithms. In this part, we can infer that the given scalability and storage optimization solutions are capable of resolving these problems. This is the first approach to solves the both problem.

The proposed scheme and its consensus algorithm would be able to solve scalability and growing blockchain size problems along with the security of the blockchain.

5.2 Future Work

The mini-shard scheme and the proposed algorithm still have some incomplete parts and issues that have to solve in the future. The account tree which store balances of the address must maintain by each node in the network. The size of the account tree should remain constant and it has to design such a way so that it would able to handled by every node in the network.

In the PoD algorithm, a slot of a round creates a block if the block gets 2/3 votes from validators. There may create a stuck situation if the block doesn't get 2/3 votes. It would be a problem if a block stacked in a slot, hence all mini-shard chains will not sync with each other. There is a proper explanation needed for how do malicious transactions would be detected?

By overcoming these limitations, a secure, scalable and lightweight blockchain can be developed.

References

[1] [Online]. Available: https://statoshi.info/d/000000006/transactions?orgId=1 (cit. on p. 6).

[2] *Bitcoin scalability problem*, May 2021. [Online]. Available: https://en.wikipedia.org/wiki/Bitcoin_scalability_problem (cit. on p. 6).

[3] K. L., *The blockchain scalability problem & the race for visa-like transaction speed*, Jul. 2019. [Online]. Available: https://towardsdatascience.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44 (cit. on p. 6).

[4] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2008. [Online]. Available: https://bitcoin.org/en/bitcoin-paper (cit. on pp. 11, 13, 27).

[5] V. Buterin *et al.*, 'A next-generation smart contract and decentralized application platform,' *white paper*, vol. 3, no. 37, 2014 (cit. on p. 12).

[6] V. Buterin, *The beacon chain*, Dec. 2020. [Online]. Available: https://ethereum.org/en/eth2/beacon-chain/ (cit. on pp. 12, 14, 18, 20).

[7] A. V. Corral, *What is sharding? here's how it works.* [Online]. Available: https://www.codementor.io/blog/sharding-ethereum-5q1k9s4kip (cit. on p. 12).

[8] J. Bruce, 'The mini-blockchain scheme,' *White paper*, 2014 (cit. on pp. 13, 18, 20).

[9] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, 'A review on consensus algorithm of blockchain,' in *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, IEEE, 2017, pp. 2567–2572 (cit. on pp. 13, 14).

[10] I. Jalal, Z. Shukur and K. A. A. Bakar, 'A study on public blockchain consensus algorithms: A systematic literature review,' 2020 (cit. on pp. 13, 14, 16, 31).

[11] V. Saini, 'Consensuspedia: An encyclopedia of 30+ consensus algorithms,' *Hackernoon [online]. Boston (MA): Hackernoon*, 2018 (cit. on p. 14).

[12] *Proof of work vs. proof of stake: What's the difference?* Oct. 2019. [Online]. Available: https://blockdaemon.com/blog/proof-of-work-vs-proof-of-stake-whats-the-difference/ (cit. on p. 14).

[13] D. Mazieres, 'The stellar consensus protocol: A federated model for internet-level consensus,' *Stellar Development Foundation*, vol. 32, 2015 (cit. on p. 15).

[14] M. Kim, Y. Kwon and Y. Kim, 'Is stellar as secure as you think?' In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, 2019, pp. 377–385 (cit. on p. 15).

[15] D. Schwartz, N. Youngs, A. Britto *et al.*, 'The ripple protocol consensus algorithm,' *Ripple Labs Inc White Paper*, vol. 5, no. 8, p. 151, 2014 (cit. on p. 16).

[16] J. Kwon, 'Tendermint: Consensus without mining,' *Draft v. 0.6, fall*, vol. 1, no. 11, 2014 (cit. on p. 16).

[17] W.-K. Fu, Y.-S. Lin, G. Campagna, C.-T. Liu, D.-Y. Tsai, C.-H. Mei, E. Y. Chang, S.-W. Liao and M. S. Lam, 'Soteria: A provably compliant user right manager using a novel two-layer blockchain technology,' in *2020 IEEE Infrastructure Conference*, IEEE, 2020, pp. 1–10 (cit. on p. 17).

[18] *Shard chains*. [Online]. Available: `https://ethereum.org/en/eth2/shard-chains/` (cit. on p. 18).

[19] Z. Ren, *What does "scalability" really mean in blockchain?* May 2019. [Online]. Available: `https://medium.com/vechain-foundation/what-does-scalability-really-mean-in-blockchain-b8b13b3181c6` (cit. on p. 29).