SCALABILITY ANALYSIS OF BLOCKCHAIN NETWORKS WITH GRADINGSHARD PROTOCOL: A PERFORMANCE EVALUATION

by

Saeed Ullah

In the partial fulfillment of the requirements

for the degree
Master of Philosophy

Department of Electronics
Quaid-i-Azam University Islamabad
Pakistan.
2021-2023

Certificate

It is certified that the work presented in this dissertation is accomplished by Saeed Ullah under my supervision at Quaid-i-Azam University, Islamabad, Pakistan.

Supervisor:

Dr. Hasan Mahmood
Professor
Department of Electronics
Quaid-i-Azam University, Islamabad, Pakistan.

Submitted through:

Prof. Dr. Qaisar Abbas Naqvi
Chairman
Department of Electronics
Quaid-i-Azam University, Islamabad, Pakistan.

Acknowledgements

I would like to express my deepest gratitude and appreciation to Allah, the Almighty, for His blessings, guidance, and mercy throughout this research journey. His unwavering support and divine wisdom have been instrumental in the successful completion of this MPhil thesis.

I am also profoundly grateful to my family for their unwavering love, encouragement, and understanding. Their constant support and belief in my abilities have been a source of strength and motivation. I am indebted to my parents, who have always been my pillars of support, for their sacrifices and continuous prayers. Their guidance and words of wisdom have shaped my character and instilled in me a sense of determination and perseverance.

I extend my sincere appreciation to my supervisor, Dr. Hasan Mahmood, for their invaluable guidance, expertise, and encouragement throughout this research endeavor. Their insightful feedback, constructive criticism, and commitment to excellence have been instrumental in shaping the direction of this thesis.

I would also like to express my gratitude to Prof. Dr. Qaisar Abbas Naqvi and all the faculty members Department of Electronics, whose knowledge, expertise, and passion for research have enriched my academic journey. Their dedication to fostering an environment of intellectual growth and scholarly excellence has had a profound impact on my development as a researcher.

Lastly, I am truly grateful to everyone who has played a part in this journey, and I pray that my work contributes positively to the field of knowledge.

Saeed Ullah

Dedicated To

My beloved Parents

Abstract

In this work, we explore the Gradingshard Protocol and present an innovative approach aimed at overcoming the throughput limitations of blockchain technology. With blockchain's rapid growth, the transaction throughput is of a critical concern for widespread adoption. The Gradingshard Protocol introduces a sharding mechanism that partitions the network into smaller subsets called shards, distributing the transaction load across independent sub-networks. This thesis provides a comprehensive overview of existing scalability challenges and traditional solutions, paving the way for Gradingshard's introduction. The protocol's architecture, consensus mechanism, and security aspects are thoroughly analyzed. Simulation experiments demonstrate the potential to significantly increase transaction processing capacity, making it an attractive solution for real-world applications. We show that Gradingshard is a promising avenue for enhancing blockchain transactions throughput and scalability.

Contents

Certificate ii
Acknowledgements iii
Abstract v
List of Figures ix
List of Abbreviations x

1 Introduction **1**
1.1 History of Blockchain 2
1.1.1 Predecessors to Blockchain (1991 - 2008) 2
1.1.2 Bitcoin Whitepaper (2008) 3
1.1.3 Bitcoin's Genesis Block (2009) 3
1.1.4 Growth of Bitcoin (2009 - 2013) 3
1.1.5 Introduction of Altcoins (2011 - 2013) 3
1.1.6 Ethereum and Smart Contracts (2015) 4
1.1.7 Blockchain Applications (2016 - Present) 4
1.1.8 Research and Development (Ongoing) 4
1.2 Types of Blockchain Technology 4
1.2.1 Public Blockchain 4
1.2.2 Private Blockchain 5
1.2.3 Consortium Blockchain 5
1.3 Background 5
1.4 Problem Statement 6
1.5 Motivation 6
1.6 Research Objectives 7
1.7 Approach 7
1.8 Thesis Structure 8

2 Literature Review **10**
2.1 Scalability and Throughput Limitations 10
2.1.1 Scalability 10
2.1.2 Throughput Limitations 10
2.1.3 Network Congestion 11
2.1.4 Energy Consumption 11
2.2 Existing solutions 11
2.2.1 Sharding 11
2.2.2 Layer-2 Scaling Solutions 12
2.2.3 Off-Chain Transactions 12
2.2.4 Consensus Mechanism Optimization 12
2.2.5 Sidechains 12
2.2.6 Parallel Processing 12
2.3 Related Work 13

3 The Gradingshard Protocol **17**
3.1 Introduction 17
3.2 Network Sharding 17
3.3 VRF_POS Algorithm 19
3.4 Gradingshard Nodes 20
3.5 Implementation of Network Sharding Approach 20
3.6 Security Evaluation 21
3.7 Evaluation of Network Sharding Efficiency 23

4 Transaction Sharding **24**
4.0.1 Introduction 24
4.1 The Foundational Framework 25
4.2 Transaction Sharding Algorithm 27
4.3 Comprehensive Blockchain Architecture 28
4.4 Security Evaluation 29
4.4.1 Security Considerations for Transaction Sharding . . . 29
4.5 Transaction Throughput 30

5 Implementation **32**
5.1 Improvement 36

6 Conclusion **41**

7 Future Work **43**

Bibliography **43**

List of Figures

1.1 Blockchain 2

3.1 The GradingShard model, comprising four shards with individual identifiers. Each shard contains a leader node, a first-level node, and multiple second-level nodes. 18
3.2 Probability Distribution being Attacked 22

4.1 Transaction Sharding Comprising Four Shards 26
4.2 Transaction Sharding Utilizing an Account-based System . . . 27
4.3 Block structure 29
4.4 Blockchain structure 30

5.1 Transaction Volume and Transaction Processing Overhead . . 34
5.2 Number of Sharding and Transaction Processing Time 35
5.3 Number of Shards and Transaction Processing Overhead . . . 36
5.4 Transaction Volume and Transaction Processing Overhead . . 37
5.5 Number of Shards and Transaction Processing Overhead . . . 38
5.6 Number of Shards and Transaction Processing Overhead . . . 39

List of Abbreviations

Acronym	Description
PoW	Proof of Work
PoS	Proof of Stack
TPS	Transactions per second
BFT	Byzantine Fault Tolerant
PoA	Proof of Authority
VRF	Verifiable Random Function

Chapter 1

Introduction

Blockchain technology is recognized for its use of nodes, which are computers connected to the network, responsible for maintaining and validating the distributed ledger system. Every transaction is organized into a "block", and subsequently, these blocks are interconnected in a chronological sequence, forming an immutable chain [1]. This structure ensures the security and integrity of the data stored in the blockchain.

One of the key features of blockchain technology is its decentralization, meaning no central authority or intermediary is controlling the system [See Figure 1]. Instead, consensus mechanisms are used to validate transactions and reach an agreement on the state of the ledger across the network. This decentralization ensures transparency and reduces the risk of single points of failure or malicious attacks.

Blockchain is most famously associated with cryptocurrencies, such as Bitcoin [2] and Ethereum [3]. In these networks, transactions are validated by "miners" or "validators" through processes like Proof-of-Work (PoW) [4] or Proof-of-Stake (PoS) [5]. Once a transaction is confirmed, it is added to the blockchain, making it permanent and tamper-proof.

Beyond cryptocurrencies, blockchain technology has broader applications. It is increasingly being used in various industries to provide transparency, security, and efficiency. Some of the notable applications include supply chain management [6], healthcare [7] [8], voting systems [9], smart contracts [10], and decentralized finance (DeFi) [11] [12].

Blockchain technology offers numerous advantages, such as increased security through encryption and immutability, reduced transaction costs by eliminating intermediaries, and improved transparency due to public visibil-

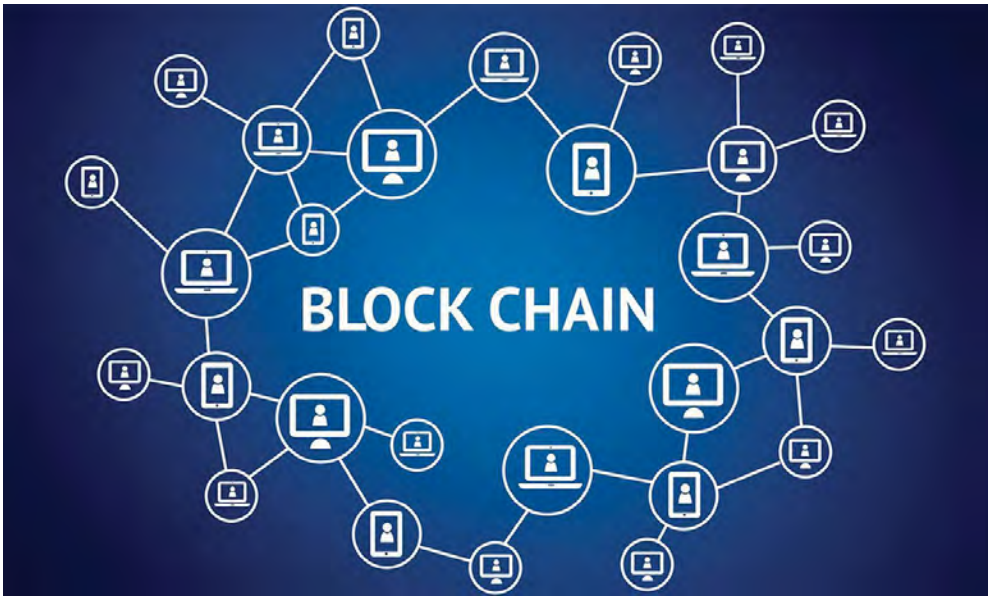

Figure 1.1: Blockchain

ity of the ledger. However, challenges remain, including scalability, energy consumption, regulatory concerns, and interoperability with existing systems.

Overall, blockchain technology represents a significant shift in the way data is stored, shared, and managed. Its potential to disrupt various industries and improve existing systems makes it a compelling area of research and development. As the technology continues to evolve, its impact on society is likely to grow, shaping the future of digital interactions and transactions.

1.1 History of Blockchain

The history of blockchain technology can be traced back to the early 1990s, but it gained significant prominence with the introduction of Bitcoin in 2008 [13]. Here is a brief overview of the key milestones in the history of blockchain:

1.1.1 Predecessors to Blockchain (1991 - 2008)

The foundational concepts of blockchain can be traced back to the early 1990s when researchers Stuart Haber and W. Scott Stornetta proposed a

cryptographically secured chain of blocks to timestamp digital documents, ensuring their immutability and preventing backdating. However, their work did not lead to the development of a practical system at that time.

1.1.2 Bitcoin Whitepaper (2008)

In October 2008, an anonymous person or group using the pseudonym Satoshi Nakamoto published the Bitcoin whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" [14]. This groundbreaking paper introduced the concept of a decentralized, peer-to-peer electronic cash system that leveraged blockchain technology to achieve consensus without relying on centralized intermediaries.

1.1.3 Bitcoin's Genesis Block (2009)

On January 3, 2009, Nakamoto mined the first block of the Bitcoin blockchain, known as the "genesis block" [15] or "block 0". This marked the official launch of the Bitcoin network, and the blockchain began recording the first transactions.

1.1.4 Growth of Bitcoin (2009 - 2013)

Bitcoin gradually gained popularity within the cypherpunk and cryptography communities. Early adopters and enthusiasts began mining and using Bitcoin for transactions. In May 2010, the first real-world Bitcoin transaction occurred when Laszlo Hanyecz famously purchased two pizzas for 10,000 BTC. The price of Bitcoin remained relatively low during this period.

1.1.5 Introduction of Altcoins (2011 - 2013)

As the interest in blockchain and cryptocurrencies grew, developers started creating alternative cryptocurrencies, often referred to as "altcoins". Litecoin, a peer-to-peer cryptocurrency that aimed to improve upon Bitcoin's shortcomings, was introduced in October 2011, becoming one of the first successful altcoins.

1.1.6 Ethereum and Smart Contracts (2015)

Ethereum, proposed by Vitalik Buterin in late 2013 and developed by a team of developers, was launched in July 2015. Ethereum introduced the concept of "smart contracts", enabling programmable, self-executing contracts without the need for intermediaries [16]. This innovation opened up a wide range of decentralized applications (dApps) beyond simple peer-to-peer transactions.

1.1.7 Blockchain Applications (2016 - Present)

Blockchain technology expanded beyond cryptocurrencies, with various industries exploring its potential. Companies and organizations began exploring blockchain for supply chain management, identity verification, voting systems, decentralized finance (DeFi), and more. Additionally, blockchain consortia and partnerships formed to develop enterprise-grade blockchain solutions.

1.1.8 Research and Development (Ongoing)

The blockchain space continues to see active research and development efforts. Projects are focused on scalability solutions, interoperability between blockchains, privacy enhancements, and the integration of blockchain technology with emerging technologies like the Internet of Things (IoT) and artificial intelligence (AI).

1.2 Types of Blockchain Technology

The major types of blockchain technology can be categorized based on their underlying consensus mechanisms, permission levels, and use cases. Here are the main types:

1.2.1 Public Blockchain

Public blockchains are open and permissionless networks accessible to anyone. They allow anyone to participate as nodes, mine (for PoW-based blockchains), and submit transactions without needing approval. Public

blockchains prioritize decentralization and transparency, making them suitable for cryptocurrencies and open-source projects. Examples include Bitcoin and Ethereum.

1.2.2 Private Blockchain

Private blockchains, also known as permissioned blockchains, restrict access and participation to authorized entities. Permission to join the network is granted by an entity controlling the blockchain, often for businesses or consortiums. Private blockchains offer enhanced privacy and are typically used for enterprise applications where data access needs to be restricted. They are more suitable for cases where trust between participants is already established.

1.2.3 Consortium Blockchain

Consortium blockchains are a hybrid model that combines features of both public and private blockchains. They are controlled by a group of pre-approved entities, such as businesses or organizations, forming a consortium. While participation is restricted, the consensus mechanism may vary between public and private models. Consortium blockchains are suitable for use cases that require both decentralization and restricted access.

1.3 Background

Blockchain technology has emerged as a groundbreaking innovation, revolutionizing various industries by offering decentralized, secure, and transparent solutions. Its immutable and distributed ledger system has the potential to transform financial transactions, supply chain management, healthcare, and other sectors. However, as the adoption of blockchain technology continues to grow, significant challenges related to scalability and throughput have emerged.

Scalability refers to a blockchain network's ability to handle an increasing number of transactions and users without compromising its performance. Blockchain's inherent design, where every participant maintains a copy of the entire ledger, can lead to bottlenecks as the network scales. This results in limited throughput, impacting the number of transactions that the network

can process per second. As more users and applications onboard, the need for a scalable solution becomes imperative for the widespread adoption of blockchain technology.

1.4 Problem Statement

The primary challenge addressed in this research is the limitation of throughput in blockchain networks. As blockchain applications continue to expand, the existing solutions, such as increasing block sizes or employing off-chain scaling techniques, have shown limitations and trade-offs in maintaining decentralization and security. Therefore, there is a need to explore innovative approaches that can enhance blockchain throughput while preserving the core principles of decentralization, security, and transparency.

1.5 Motivation

The motivation for this thesis, "Exploring Gradingshard Protocol [17] for Enhancing Throughput in Blockchain Technology," stems from the growing need for scalable and efficient blockchain solutions. As blockchain technology gains widespread adoption across various industries, it faces inherent limitations concerning throughput and scalability. These limitations hinder blockchain's ability to handle a high volume of transactions, resulting in slower processing times and higher fees.

The Gradingshard Protocol has emerged as a promising solution to address these challenges. By employing sharding, the protocol aims to parallelize transaction processing, thereby enhancing blockchain throughput and reducing transaction latency. However, despite its potential, the Gradingshard Protocol is still relatively new, and its effectiveness under different network conditions needs comprehensive exploration.

This thesis seeks to provide a thorough investigation into the Gradingshard Protocol's capabilities and limitations, aiming to contribute to the broader understanding of sharding-based solutions in blockchain technology. By conducting an in-depth analysis, simulation experiments, and security evaluation, the research aims to shed light on how the Gradingshard Protocol can positively impact blockchain throughput and transaction speeds while ensuring network security and decentralization.

The findings of this thesis are expected to provide valuable insights to blockchain developers, researchers, and industry practitioners. The results can inform the development of more scalable and efficient blockchain protocols, fostering innovation and growth in the blockchain ecosystem. Additionally, the research aims to help decision-makers in various industries make informed choices when considering the implementation of blockchain technology, especially in use cases that demand high throughput and quick transaction processing.

Ultimately, the motivation behind this thesis lies in contributing to the advancement of blockchain technology, making it a more viable solution for real-world applications, and unlocking its potential to revolutionize industries by enhancing efficiency, security, and overall user experience. Through a comprehensive exploration of the Gradingshard Protocol, this research endeavors to pave the way for a more scalable, inclusive, and sustainable blockchain future.

1.6 Research Objectives

The research objectives encompass understanding existing challenges in blockchain scalability and throughput limitations, analyzing conventional solutions for enhancing blockchain throughput and identifying their shortcomings, exploring the Gradingshard Protocol as an alternative approach to improving blockchain throughput through sharding, evaluating the protocol's performance in terms of throughput and latency under various network conditions, examining its security implications and proposing mitigation strategies against potential vulnerabilities, investigating the economic aspects of the Gradingshard Protocol, including incentives and governance mechanisms, and identifying practical implementation challenges and potential future developments of the protocol.

1.7 Approach

The approach for this research involves utilizing Python as the primary coding language to implement and evaluate the sharding method in blockchain technology. Python offers a powerful and versatile environment, making it well-suited for developing blockchain systems and conducting simulations.

The research will focus on implementing the sharding technique, where the blockchain network will be partitioned into smaller shards to facilitate parallel processing of transactions. Through Python coding, the sharding algorithm will be integrated into the blockchain's consensus mechanism, enabling the distribution of workload and enhancing overall throughput. Extensive simulations will be conducted to measure the performance of the sharded blockchain, comparing it with traditional non-sharded approaches. The evaluation will focus on key metrics such as transaction processing speed, scalability, and network security. The results obtained from the Python-based implementation and evaluation will contribute to a deeper understanding of the impact of sharding on blockchain performance, thus guiding the development of more efficient and scalable blockchain solutions.

1.8 Thesis Structure

The structure of the thesis is as follows:

Chapter 1, provides an introduction to the Blockchain, presenting the history of blockchain, types of blockchain, background, problem statement, motivation, research objectives, approach, and thesis organization.

Chapter 2, conducts a comprehensive literature review on scalability and throughput, existing throughput solutions, and related studies on sharding in blockchain.

Chapter 3, goes through to the Gradingshard Protocol, network sharding, covering Verifiable Random Function - Proof of Stake (VRF_POS) algorithm, explanation of nodes, implementation of network sharding approach, security evaluation, and evaluation of network sharding efficiency.

Chapter 4, covers transaction sharding, foundational framework, simulation setup, transaction sharding algorithm, comprehensive blockchain architecture, security evaluation of transaction sharding, and transaction throughput.

Chapter 5, presents the implementation of the Gradingshard Protocol in Python, followed by a performance evaluation through throughput, and will show the results through Python programming according to the data.

In Chapter 6, we conclude this thesis by addressing the throughput problems in blockchain technology and proposing the Gradingshard protocol as a solution. Through rigorous analysis and experimentation, we demonstrate

the protocol's effectiveness in enhancing transaction throughput and revolutionizing blockchain scalability and efficiency.

Chapter 7 The final chapter explores into future directions and possible enhancements to the Gradingshard protocol. It identifies areas of improvement to further enhance transaction throughput and scalability. The chapter concludes with an outlook on the potential impact of the proposed sharding protocol in advancing blockchain technology.

By organizing the thesis in this manner, readers can gain a thorough understanding of the challenges posed by low transaction throughput in conventional blockchains, the proposed Gradingshard protocol, and the experimental evaluation. Furthermore, the future work section provides insights into the ongoing research and possibilities for further advancements in sharding technology.

Chapter 2

Literature Review

2.1 Scalability and Throughput Limitations

Blockchain scalability and throughput limitations are significant challenges that hinder the widespread adoption and practical implementation of blockchain technology in various industries. These limitations arise due to the inherent design and architecture of traditional blockchain networks, such as Bitcoin and Ethereum [18], which operates on a linear and sequential transaction processing system.

2.1.1 Scalability

Scalability refers to a blockchain network's ability to handle an increasing number of transactions without compromising its performance. Traditional blockchains have a limited capacity to process transactions per second (TPS) [19], leading to network congestion during peak times. As the number of participants and transactions grows, the blockchain faces challenges in maintaining quick confirmation times and low transaction fees [20]. The scalability issue becomes more pronounced as the network reaches its capacity, impacting the user experience and hindering the adoption of blockchain for large-scale applications.

2.1.2 Throughput Limitations

Throughput is the rate at which a blockchain can process transactions within a given time frame. Traditional blockchain networks face throughput limita-

tions due to their consensus mechanisms, such as PoW or PoS [19]. These approaches necessitate extensive computational resources or restrict the number of validators, resulting in limited transaction processing speed [21]. As a consequence, transaction times are prolonged, leading to delays in confirmation and settlement, particularly during periods of high network activity.

2.1.3 Network Congestion

When blockchain networks experience a surge in transaction activity, they can become congested [22], leading to slower transaction processing and higher fees. As more transactions compete for inclusion in the limited block space, users may need to offer higher transaction fees to prioritize their transactions, resulting in an inefficient and expensive user experience.

2.1.4 Energy Consumption

Some consensus mechanisms, such as PoW, require significant computational power and energy consumption for validating transactions and creating new blocks [23]. The energy-intensive nature of these mechanisms contributes to environmental concerns and hinders the scalability of public blockchains.

2.2 Existing solutions

Several existing solutions [24] [25] [26] [27] [28] [29] have been proposed and implemented to enhance blockchain technology and address its scalability, throughput, and other limitations. These solutions aim to enhance the performance, efficiency, and usability of blockchain networks. Some of the key existing solutions include:

2.2.1 Sharding

Sharding is a technique that involves dividing a blockchain network into smaller, manageable subsets called shards [30]. Each shard can process transactions independently, allowing for parallel transaction processing and increasing overall throughput. Sharding [31] helps mitigate the scalability issues faced by traditional blockchains and improves transaction speeds.

2.2.2 Layer-2 Scaling Solutions

Layer-2 scaling solutions are protocols built on top of existing blockchains to offload some of the transaction processing to secondary layers. Examples include the Lightning Network for Bitcoin and the Raiden Network for Ethereum [32]. These solutions [33] [28] [29] enable faster and cheaper transactions by reducing the burden on the main blockchain.

2.2.3 Off-Chain Transactions

Off-chain transactions involve moving some transactions off the main blockchain to be processed privately between parties. Once the off-chain transactions are completed, the final result is recorded on the main blockchain, reducing congestion and improving throughput [22].

2.2.4 Consensus Mechanism Optimization

Existing blockchains often use energy-intensive consensus mechanisms like PoW. Transitioning to more efficient consensus mechanisms like PoS reduces energy consumption, improves scalability, and allows for faster block validation [21].

2.2.5 Sidechains

Sidechains are separate blockchains that are interoperable with the main blockchain [34]. They enable the execution of specific functions or smart contracts off the main chain, which can improve overall network performance and scalability [35].

2.2.6 Parallel Processing

Some blockchain networks are exploring techniques that enable parallel processing of transactions, allowing multiple transactions to be validated simultaneously, leading to improved throughput [36].

These existing solutions [24] [25] [26] [27] [28] [29] demonstrate ongoing efforts to enhance blockchain technology and make it more adaptable to real-world use cases. Each solution addresses specific challenges, and their

combination or further developments may pave the way for a more scalable, efficient, and versatile blockchain ecosystem.

2.3 Related Work

In recent times, scholars and experts have introduced the concept of sharding as a protocol to enhance the capabilities of blockchain technology. Sharding has emerged as a potential solution to address the scalability limitations faced by traditional blockchain networks [37]. This innovative approach aims to improve transaction processing speeds, reduce confirmation times, and increase the overall capacity of blockchain systems. By dividing the network into smaller, manageable subsets called shards, sharding enables parallel transaction processing, significantly boosting the network's throughput [30]. Through this novel protocol, researchers seek to revolutionize the blockchain landscape and unlock new possibilities for real-world applications of this transformative technology.

Omniledger [25] introduces a sharding approach that combines PoW and a Byzantine fault tolerant (BFT) hybrid consensus protocol. The blockchain network is comprised of an identity chain and multiple shard sub-chains. Validators are distributed in a decentralized manner across these shard sub-chains, and they achieve consensus via an efficient cross-shard protocol. By leveraging this innovative combination, Omniledger achieves a significant throughput of 1674 transactions per second (TPS) with just four shards. Monoxide [26] has put forward a concept called consolidated mining, which involves sharing mining computing power across different segments. Nonetheless, a valid concern arises regarding the possibility of power concentration among nodes equipped with professional mining facilities in this approach. Ethereum 2.0 [27] introduces the Shasper sharding protocol, which aims to enhance scalability by dividing the network into smaller shards. These shards are agreed upon by the continuously updated verifiers, each of whom is responsible for storing and validating transactions within specific shards. However, this approach comes with some challenges. Verifiers are required to store data from multiple shards, resulting in increased storage requirements and communication overhead.

RapidChain [28] is an innovative public blockchain protocol that adopts sharding to address scalability and security concerns. Unlike previous sharding-based protocols, RapidChain is resilient to Byzantine faults, meaning it can

tolerate up to a 1/3 fraction of participants acting maliciously. It accomplishes full sharding of communication, computation, and storage overhead without requiring any trusted setup. Through the use of optimal consensus algorithms, efficient block pipelining, and cross-shard verification techniques, RapidChain demonstrates impressive performance, processing over 7,300 transactions per second with a confirmation delay of just 8.7 seconds in a network of 4,000 nodes. The protocol's high robustness and scalability are substantiated by thorough empirical evaluations, positioning RapidChain as a promising solution for secure and scalable large-scale blockchain networks.

In Elastico [29], shard transactions are validated using a global ledger, but the protocol lacks a security mechanism to guarantee the atomicity of cross-shard verification. This means that if a cross-shard transaction is declined for any reason, it may result in a deadlock situation where further progress becomes impossible. Such a deadlock scenario could lead to potential financial losses for participants involved in the transaction. In essence, the absence of a robust atomicity guarantee in the cross-shard verification process poses a significant risk to the stability and reliability of the blockchain network.

Chainspace [38] introduces a sharding mechanism specifically tailored for smart contracts. However, this implementation comes with a drawback - the achieved throughput is lower than 400 transactions per second (TPS).

A PoS-based scalable blockchain protocol that addresses the scalability challenge. The protocol utilizes a PoS consensus mechanism and a sharding protocol [39]. In place of processing transactions across the entire network, transactions are segmented into transaction shards, while the network is divided into network shards. These network shards concurrently process transaction shards, creating intermediate blocks that are merged to form the ultimate block with a recorded timestamp on the blockchain. Through experiments on a simulated network of 100 Amazon EC2 instances, the protocol exhibited an average latency of around 27 seconds and a maximum throughput of 36 transactions per second for a 100-node network. The outcomes demonstrate that the proposed protocol's throughput scales with the network size, confirming its potential for scalability.

StakeCube [40] introduces a sharding approach that relies on the PoS protocol and adopts a hypercube-distributed hash table routing node for sharding strategies. The sharding method in StakeCube is determined based on routing distance calculations. However, a limitation of StakeCube's sharding method is that it does not protect against simultaneous attacks from malicious nodes targeting a shard. This vulnerability could potentially compro-

mise the security and integrity of the shard, affecting the overall robustness of the blockchain network. As a result, ensuring robust defense mechanisms against coordinated attacks remains an essential consideration in evaluating the effectiveness of StakeCube's sharding approach. Lee et al. [41] presented a sharding technique utilizing the PoS protocol, featuring fair and dynamic sharding management. In contrast to the three PoS-based sharding methods discussed earlier, Lee et al.'s approach avoids complete reliance on random sharding, thereby reducing the predictability of potential shard attacks. However, the concern arises that if an attack targets a shard, it could compromise the overall security of the whole blockchain network. Therefore, ensuring robust defense mechanisms against potential attacks is essential to maintain the security and integrity of the blockchain in the context of Lee et al.'s suggested PoS sharding method. Jiang et al. [42] introduced a reputation evaluation model to reduce the risk of malicious nodes obtaining master node status. While this model achieves an impressive throughput of 5,000 TPS with 3 shards, it also results in increased network overhead. However, it is essential to consider that with the growing number of shards, the protocol's throughput growth shows signs of diminishing, implying potential scalability limitations. As a consequence, while the reputation evaluation model successfully addresses security concerns, further investigation is necessary to assess its long-term scalability and overall network performance when operating with a larger number of shards.

In addition to the sharding systems mentioned earlier, other sharding implementations rely on different consensus protocols. BlockTree [43] presents a novel strategy for achieving a secure, scalable, and distributed ledger through the implementation of sharding. Although it introduces a distinct consensus protocol, it also alters the interconnections between blocks in the chain and schema, potentially leading to increased complexity in tracing transactions. Despite its benefits in terms of security and scalability, this reconstruction of connections introduces challenges for transaction traceability and auditing. Evaluating the trade-offs between security and traceability is crucial when considering the implementation of BlockTree as a blockchain solution. MedShard [44] employs a Proof of Authority (PoA) consensus mechanism to achieve consensus among shards, thus alleviating the complexities associated with cross-shard communication. In contrast, its adaptability is limited as the shards are determined by the entities the patient has visited previously. Despite the efforts made to address the throughput problem, each approach has its inherent limitations. In response to this, we introduce an

innovative sharding approach known as GradingShard, aiming to overcome the drawbacks of previous approaches and offer an innovative solution to the scalability and throughput challenges in blockchain technology.

GradingShard [17] introduces a comprehensive sharding approach comprising network sharding and transaction sharding. Network sharding divides the blockchain network into multiple subnetworks, enabling parallel processing of transactions within each subnetwork. On the other hand, transaction sharding categorizes and distributes transactions across various network shards. This unique combination of sharding mechanisms enhances both the security and throughput of the blockchain significantly. Empirical testing demonstrates that the GradingShard protocol can process an impressive 500,000 transactions in just 5 seconds, showcasing its potential to significantly improve the performance and efficiency of blockchain networks.

Chapter 3

The Gradingshard Protocol

3.1 Introduction

The Gradingshard Protocol is a novel approach to enhancing blockchain throug-hput through the implementation of sharding. It aims to address the scalability limitations faced by traditional blockchains by partitioning the network into smaller, manageable subsets known as shards. Each shard operates independently, handling a portion of the total transactions, and collectively, the shards form the complete blockchain. The protocol is designed to achieve higher transaction processing speeds, reduced confirmation times, and increased overall network capacity.

3.2 Network Sharding

In this section, we present the fundamental concept of network sharding and its importance in ensuring the security and performance of blockchain networks. As blockchain networks grow, the presence of malicious nodes poses a significant threat to the overall integrity of the system. If a significant number of malicious nodes manipulate a shard, it could fail the entire blockchain. In order to address this security concern, we propose a novel approach called the random, sharding strategy, aimed at reducing the likelihood of malicious node attacks on the network.

The network sharding process involves dividing the blockchain network into several subnetworks, known as shards. Each shard is responsible for processing specific subsets of blockchain transactions. By doing so, we achieve

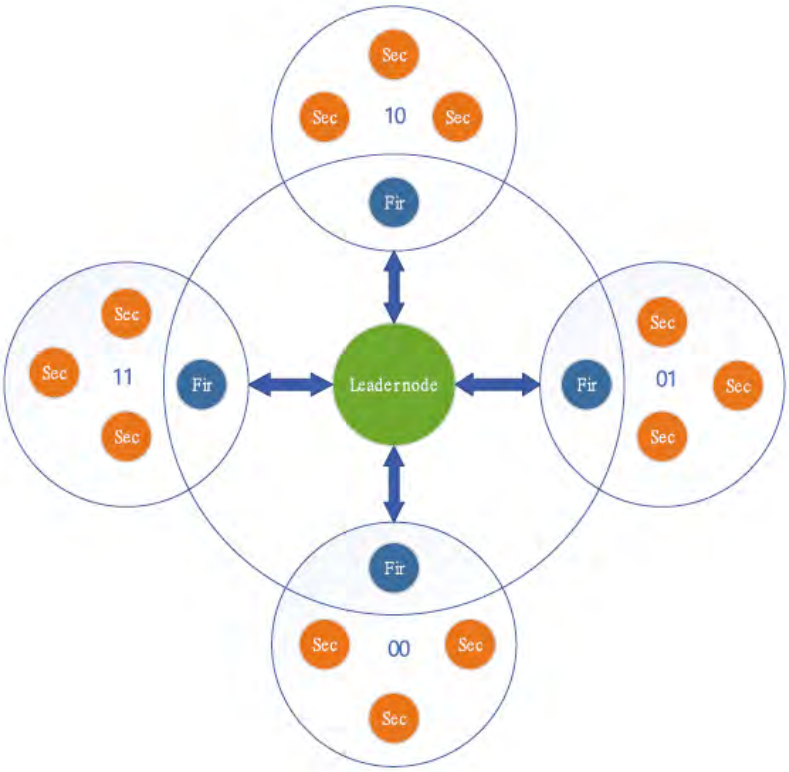

Figure 3.1: The GradingShard model, comprising four shards with individual identifiers. Each shard contains a leader node, a first-level node, and multiple second-level nodes.

parallel processing of transactions, which can significantly enhance the overall throughput and scalability of the blockchain.

Fig 3.1 illustrates the network sharding model employed in GradingShard. The model comprises four distinct shards, with each shard featuring a single first-level node and numerous second-level nodes. Notably, the sole node representing the entire blockchain network is known as the leader node. In the forthcoming sections, we will delve into the significance and functionality of these nodes, providing a comprehensive explanation of their roles within the GradingShard protocol. By explaining the characteristics and interactions of these nodes, we aim to offer a clear understanding of the inner workings of the GradingShard network sharding model and its contribution to enhancing blockchain throughput and scalability.

3.3 VRF_POS Algorithm

The Verifiable Random Function - Proof of Stake (VRF_POS) algorithm is a cryptographic protocol used in blockchain networks to achieve secure and random leader selection in a PoS consensus mechanism. It allows for the deterministic selection of a block proposer (leader) for a given block in a PoS-based blockchain, ensuring fairness and preventing manipulation.

The VRF_POS algorithm utilizes a Verifiable Random Function (VRF), which is a cryptographic primitive that takes a secret key and an input as parameters and produces a random output, known as a proof. This proof can be publicly verified to ensure its validity and authenticity.

In the context of PoS consensus, the VRF_POS algorithm ensures that each node in the network can participate in the block proposal process based on its stake (the amount of cryptocurrency it holds and is willing to "stake" as collateral). Nodes with a higher stake have a greater chance of being selected as the leader to propose the next block.

The process of leader selection using VRF_POS involves the following steps:

1. **Key Generation**

   Each node generates a secret key and corresponding public key for the VRF.

2. **VRF Output Computation**

   The nodes use their secret keys and a unique identifier for the block to compute the VRF output, which includes the random proof.

3. **Broadcasting VRF Outputs**

   The nodes then broadcast their VRF outputs to the network.

4. **Verification of VRF Outputs**

   Other nodes can verify the validity of the VRF outputs using the public keys and the unique identifier. This ensures that the leader selection process is transparent and verifiable.

5. **Leader Selection**

   The node with the highest VRF output (based on the proof) is selected as the leader to propose the next block.

By utilizing the VRF_POS algorithm, blockchain networks can achieve a fair and secure leader selection process in a PoS-based consensus mechanism, providing a robust and efficient approach to achieving consensus and validating transactions on the blockchain.

3.4 Gradingshard Nodes

Participants in the network sharding and consensus process are referred to as "verifiers". They consist of three types: leader nodes, first-level nodes, and second-level nodes, each fulfilling specific roles. Leader nodes are situated outside any shard, while first-level and second-level nodes act as validators within their respective shards. The distribution of responsibilities among the different validators is as follows:

Leader Node: Responsible for verifying the sub-MerkleRoot hash result and signature provided by each first-level node in the shard. Additionally, the leader node is in charge of assembling and broadcasting the final block containing the validated transactions.

First-level Nodes: These nodes are responsible for proposing transactions and packaging transactions specific to their shard. They calculate and sign the sub-MerkleRoot hash result and actively participate in the consensus process to ensure the validity and integrity of transactions within the shard.

Second-level Nodes: These nodes play a crucial role in transmitting transactions across the network. They assist in completing the signature of the sub-MerkleRoot hash result and are responsible for creating transaction hashes. By performing these tasks, second-level nodes contribute to the efficient and secure processing of transactions within the sharding protocol.

3.5 Implementation of Network Sharding Approach

The network sharding implementation involves the utilization of VRF_POS to establish network sharding, while PoS is employed to determine the nodes' identities. The following steps outline the fundamental process of network sharding:

1. **System Initialization:** Each registered blockchain node in the network generates a pair of public key (pk) and private key (sk).

2. **VRF Algorithm for Leader Selection:** A random string (S) from the entire network, such as the height of the previous block, the overall network synchronization time, or the block hash, is used as input for the VRF algorithm. Additionally, the node's private key (sk) is considered as input for the VRF algorithm. The VRF generates a random number and maps it to the interval [0, $value$).

3. **Leader Election:** The probability of the system initializing the leader selection process is 1/1000. The node with a random number less than 1 is elected as the leader, responsible for packaging the final blocks.

4. **Network Sharding:** Assuming network sharding $M = 4$, each verifier uses y (a VRF_POS result) mod M to obtain a sharding number S_i, where S_0, S_1, S_2, and S_3 represent the shards 0, 1, 2, and 3, respectively. In S_i, nodes whose result y divided by the account capital (w) is less than 1 are classified as first-level nodes, while the rest are considered second-level nodes.

3.6 Security Evaluation

The security analysis of the GradingShard protocol focuses on the vulnerability introduced by the presence of malicious nodes within network shards. Specifically, only the first-level nodes in each shard participate in the consensus protocol. If more than 1/3 of the malicious nodes simultaneously become first-level nodes and reside in a shard, it poses a serious security risk to the entire blockchain system.

Let the blockchain network consist of n nodes, and among them, j nodes are malicious. Considering network sharding based on the prefix k of account addresses, the likelihood of a malicious node breaching a shard follows a binomial distribution, as given by Equation (1):

$$P = \binom{n}{j} \left(\frac{1}{2^k}\right)^j \left(1 - \frac{1}{2^k}\right)^{n-j} \tag{3.1}$$

For instance, assuming there are 400 first-level nodes in the blockchain network, and sharding is performed with $k = 1$, $k = 2$, $k = 3$, and $k =$

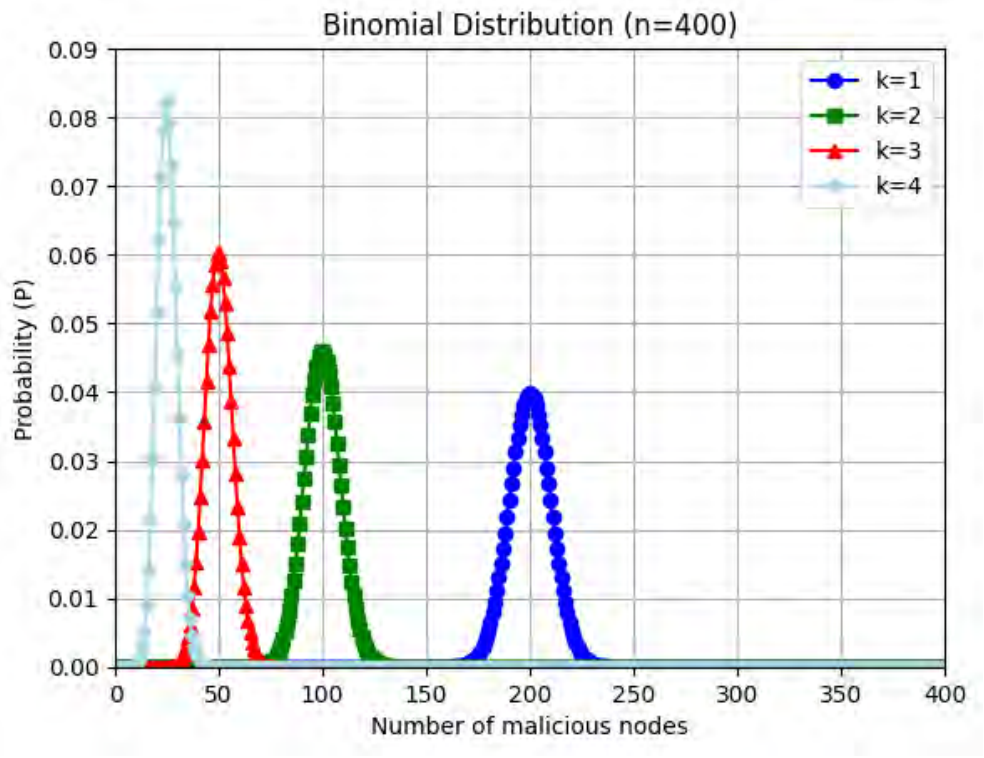

Figure 3.2: Probability Distribution being Attacked

4, resulting in 2, 4, 8, and 16 shards respectively. The probability of a malicious node attacking a shard is 0.5, 0.25, 0.125, and 0.0625 respectively, corresponding to different prefix k values.

Figure 2 illustrates the likelihood of a shard being attacked by malicious nodes. As the number of shards increases, the probability of malicious nodes concentrating on a single shard decreases, as malicious nodes follow the binomial distribution. Consequently, while a few shards may be compromised, the majority of shards remain secure. During the consensus phase, The shards affected by malicious nodes are isolated, ensuring the security of the overall blockchain network. This proactive isolation mechanism safeguards the integrity and reliability of the network by preventing any potential harm caused by malicious actors.

3.7 Evaluation of Network Sharding Efficiency

One of the critical challenges faced by traditional blockchain systems is their limited throughput scalability. In conventional setups, the throughput of a blockchain network with n mining nodes is equivalent to that of a network with 100 * n mining nodes. In order to address this limitation, we propose an innovative approach based on network sharding. In the proposed scheme, the entire blockchain network is partitioned into m shards, with each shard containing n online nodes. Each shard can process t_x transactions per unit of time, and its consensus time overhead is represented by t_0, while the time cost of network sharding is denoted by t_1. This research demonstrates that this new blockchain structure enables M transactions per unit of time, significantly surpassing the throughput *(M1)* of traditional blockchain structures

$$\frac{M}{M_1} = m \cdot \frac{t_0'}{t_0 + t_1} \tag{3.2}$$

By analyzing the efficiency of our proposed network sharding mechanism, we find that $t_1 \ll t_0$, leading to $t_0 + t_1 \approx t_0$. Consequently, the consensus time of n nodes in the blockchain network must be greater than the consensus time cost of m $(n \cdot m)$ nodes, indicating that $t_0' > t_0$.

$$\frac{M}{M_1} > m \tag{3.3}$$

Our evaluation shows that the overall throughput of the blockchain structure is determined by the following equations:

$$M = m \cdot \frac{tx}{t_0 + t_1} \tag{3.4}$$

$$M_1 = \frac{tx}{t_0'} \tag{3.5}$$

Through the proposed network sharding mechanism, we achieve a substantial increase in blockchain throughput, offering a minimum of m times improvement, where m represents the number of network shards. This advancement in scalability and throughput demonstrates the efficacy of the presented approach that enhances blockchain technology.

Chapter 4

Transaction Sharding

4.0.1 Introduction

Transaction sharding plays a pivotal role in enhancing the efficiency of blockchain networks by strategically dividing unconfirmed transactions into distinct network shards based on predefined rules. The fundamental objective behind transaction sharding is to enable parallel processing of these transactions within each shard, significantly increasing the overall throughput and scalability of the blockchain system. By distributing the transaction processing workload across multiple shards, the network can efficiently handle a larger volume of transactions simultaneously, thus reducing bottlenecks and improving overall transaction processing speed.

The process of transaction sharding involves intelligently assigning transactions to specific shards based on various factors, such as transaction type, user identity, or geographic location. This allocation ensures that each shard processes a specific subset of transactions, leading to optimized utilization of network resources and computational power. Additionally, transaction sharding minimizes the chances of contention or conflicts among transactions, as each shard operates independently and autonomously.

One of the key advantages of transaction sharding is its potential to alleviate the scalability limitations of traditional blockchain networks. As the number of transactions increases, traditional blockchain systems often experience congestion, resulting in longer confirmation times and higher transaction fees. Transaction sharding, on the other hand, offers a scalable solution by enabling the network to process multiple sets of transactions concurrently, effectively mitigating congestion and enhancing the system's overall efficiency.

Furthermore, transaction sharding promotes improved fault tolerance within the blockchain network. In the event of a failure or malicious attack on a particular shard, the rest of the network remains unaffected, ensuring that the entire blockchain system continues to function without disruption. This resilience is crucial for maintaining the integrity and reliability of blockchain networks, especially in large-scale and mission-critical applications.

Overall, transaction sharding represents a significant advancement in blockchain technology, as it addresses the challenges associated with scalability, throughput, and efficiency. By harnessing the power of parallel processing and intelligent transaction allocation, transaction sharding empowers blockchain networks to handle a substantial increase in transaction volume, opening up new possibilities for real-world applications and further driving the widespread adoption of blockchain technology.

4.1 The Foundational Framework

This research adopts a specific rule based on the address model for selecting transaction sharding. The visualization of the transaction sharding process is illustrated in Fig 4.1, which presents a schematic diagram comprising four shards. Upon the completion of subMerkleRoot generation in each shard, the first-level node broadcasts it to the leader node. Subsequently, the leader node consolidates all subMerkleRoots to construct the final Merkle root hash, leading to the creation of a new block that is subsequently released to the broader blockchain network.

If the blockchain network is divided into four shards, the transaction sharding is depicted in Fig 4.2. The diagram illustrates that based on the first two binary digits of the account number, all account transactions can be segregated into four shards, enabling parallel processing of transactions within the four distinct network shards.

For instance, an account with the first two digits “00” in its binary representation is processed by a node assigned to network shard “00”. The first-level node assigned to network shard “00” consolidates all transactions submitted by accounts with the first two binary digits “00”, forming a subMerkleRoot hash (hash00). The same process is carried out for the other shards (hash01, hash10, and hash11). Eventually, each shard’s first-level node broadcasts the subMerkleRoot hash values, i.e., hash00, hash01, hash10, and hash11. Subsequently, the leader node, elected by the network shard,

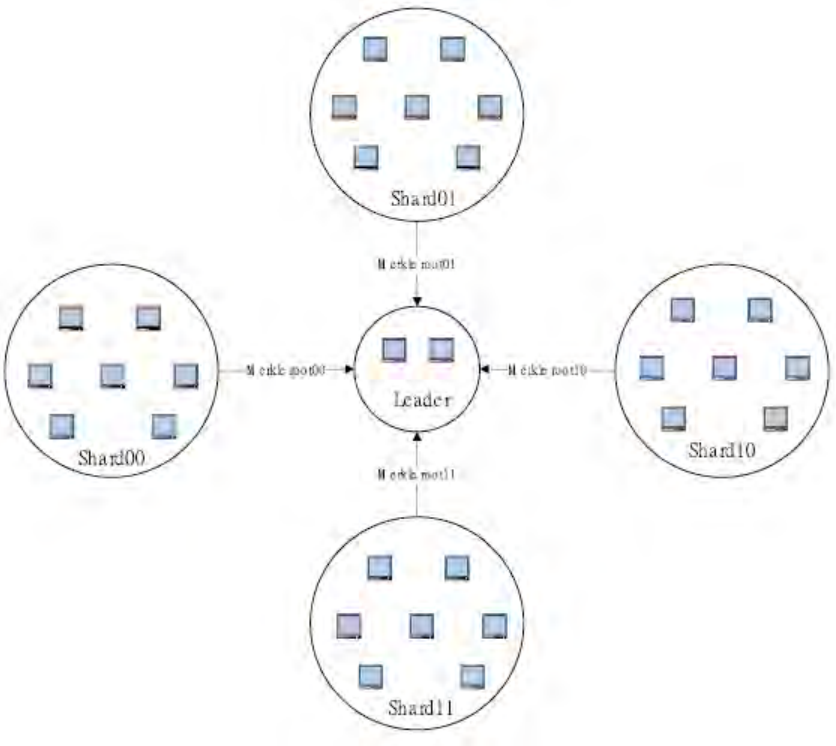

Figure 4.1: Transaction Sharding Comprising Four Shards

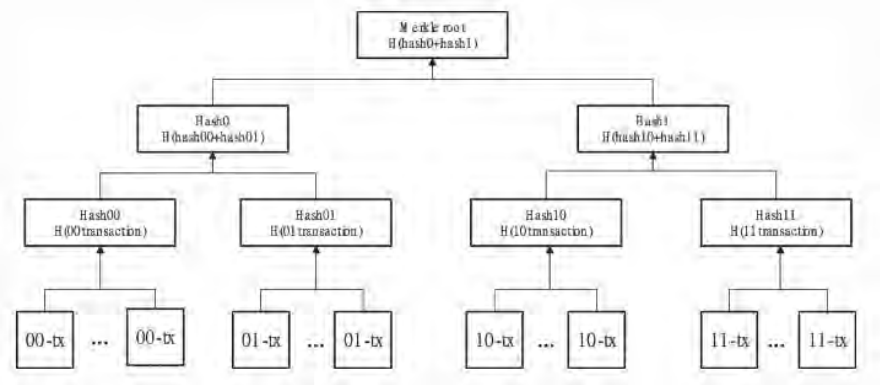

Figure 4.2: Transaction Sharding Utilizing an Account-based System

packages all the subMerkleRoot hash values to create the final MerkleRoot hash value.

4.2 Transaction Sharding Algorithm

The Transaction Sharding Algorithm is an algorithmic process used to divide unconfirmed transactions within a blockchain network into smaller, manageable subsets called shards. The goal is to achieve parallel processing of transactions across multiple shards, leading to improved efficiency and scalability of the blockchain network.

1. **Sharding Rule:** A specific rule based on the accounting system is employed to determine which shard a transaction belongs to. The rule may be based on certain properties of the transaction, such as the account number or specific attributes of the transaction data.

2. **Shard Creation:** Once the sharding rule is applied to a transaction, it is assigned to the corresponding shard based on the outcome of the rule. This process continues for all incoming transactions, effectively creating multiple shards, each responsible for processing a subset of transactions.

3. **SubMerkleRoot Generation:** Within each shard, the first-level node is tasked with gathering and consolidating all the transactions belong-

ing to that shard. These transactions are then combined to generate a SubMerkleRoot hash value, representing the contents of that shard.

4. **Broadcasting SubMerkleRoot:** Each first-level node broadcasts the SubMerkleRoot hash value it has generated to the network. This step allows the other nodes in the network to be aware of the transactions processed within their respective shards.

5. **Final MerkleRoot Hash:** The leader node, elected by the network, takes on the responsibility of collecting all the SubMerkleRoot hash values from each shard. The leader node then combines these hash values to create the final MerkleRoot hash value.

By employing the Transaction Sharding Algorithm, the blockchain network achieves the parallel processing of transactions, significantly increasing its throughput and overall efficiency. Moreover, Transaction Sharding helps alleviate the scalability challenges faced by traditional blockchain systems, paving the way for more practical and sustainable blockchain technology applications in various domains.

4.3 Comprehensive Blockchain Architecture

Once the transaction sharding process is completed within the blockchain network, the leader node assumes the responsibility of releasing the latest block. Fig 4.3 provides an overview of the block structure, while Fig 4.4 illustrates the overall blockchain structure derived from the blocks depicted in Fig 4.3. The block structure, as depicted in Fig 4.3, is composed of a block header and a block body, which together constitute a complete block. The block header comprises essential information, including the current block version number, the hash of the previous block, the timestamp, the probability value of the elected leader, and the Merkle root hash value of all transactions. Meanwhile, the block body contains the subMerkleRoot hash values of all transactions within their respective sharding. These subMerkleRoot hash values are then combined to form the final Merkle root hash value. As depicted in Fig 4.4, the blockchain is a sequence of interconnected blocks, where each block is based on the hash field of the previous block. The hash value of the previous block of each block is computed using the following formula:

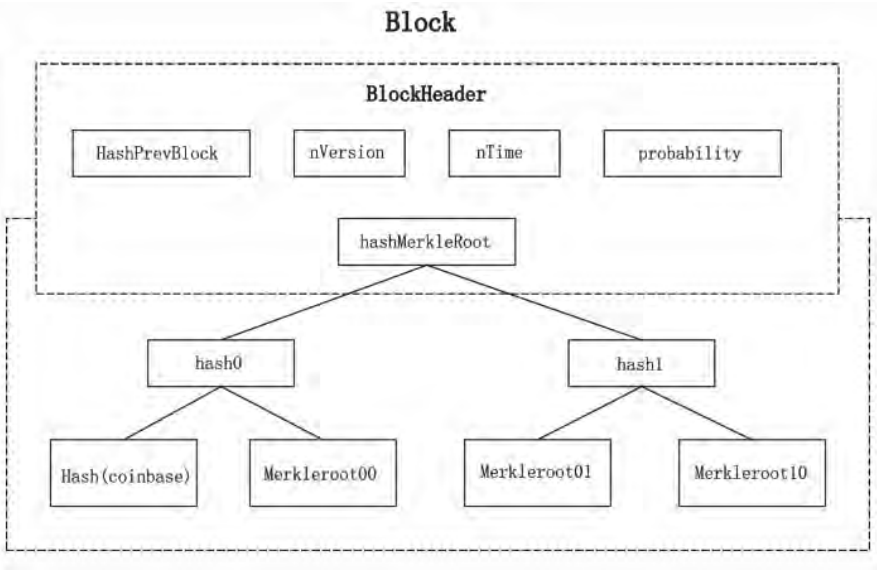

Figure 4.3: Block structure

hashPreBlock $_{i+1} = sha256(nVersion_i + hashPreBlock_i + hashMerkleRoot_i + nTime_i + probability_i)$

4.4 Security Evaluation

4.4.1 Security Considerations for Transaction Sharding

The transaction sharding mechanism proposed in this paper relies on the account's prefix to divide transactions within the same shard by consensus. This approach effectively addresses the threat of "double spending" [45], as transactions with the same prefix are handled in the same sharding, making it easier to identify and prevent such fraudulent transactions. Furthermore, this sharding scheme ensures no additional overhead is incurred across network shards, enhancing security.

In order to form a subMerkleRoot value, the transaction sharding process splits a block's Merkle root [46] hash value into multiple shards, and the leader node is not involved in verifying the transaction's validity. To safeguard the Merkle root hash value of each subtree generated by shard-

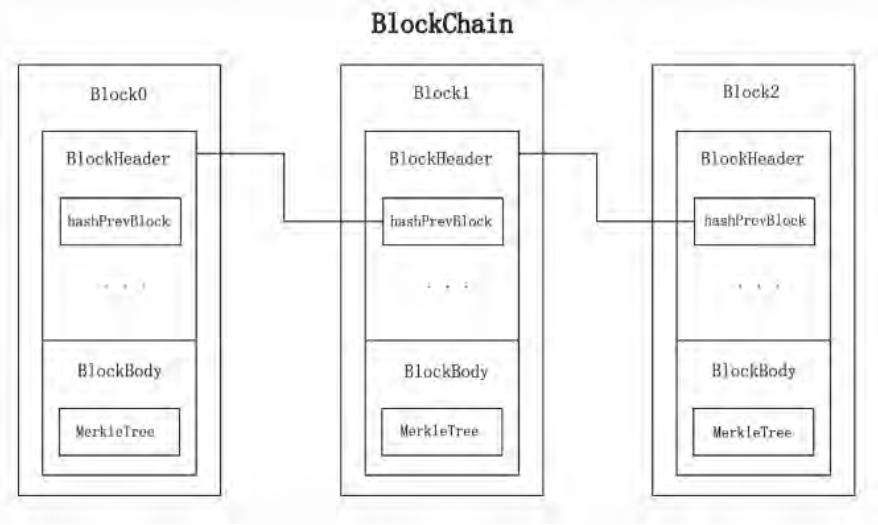

Figure 4.4: Blockchain structure

ing, a new data structure called *MerkleRoot_i* has been implemented in this thesis. This data structure ensures the integrity of *MerkleRoot_i* when first-level nodes in the same sharding conduct the consensus protocol. Even if a malicious first-level node attempts to perform an unauthorized operation on the *subMerkleRoot_i*, such as an incorrect Merkle root hash signature, the signatures of other honest first-level nodes remain unaffected.

4.5 Transaction Throughput

The transaction sharding proposed in this paper effectively addresses the issue of each node having to package all transactions. In a conventional blockchain network with N transactions at a given time, the complexity of packaging all transactions for each mining node is $M = O(n)$. In contrast, the average complexity for each mining node in the proposed transaction sharding scheme, considering M sharding in the blockchain network and parallel computation within each shard, is $M1 = O(n/m)$

$$\frac{M}{M_1} = m \tag{4.1}$$

From eq 4.1, it is evident that traditional blockchain networks experi-

ence linearly increasing transaction packaging complexity when conducting transaction sharding.

Chapter 5

Implementation

In order to assess the effectiveness of the presented sharding protocol, we conducted extensive simulations with a significant number of nodes. The experimental setup consisted of two main sections: network sharding and transaction sharding. The relevant parameters used in these experiments are listed in Table 5.1. It's important to note that all simulations were performed using Python as the programming language.

Table 5.1 presents the experimental parameters used in our research, which were crucial in evaluating the performance of the proposed sharding protocol.

Table 5.1: Experimental Parameters

Name	**Value**
Nodes in the entire network	10,000
Network sharding	16
Probability of leader election	0.0001
Number of transactions	10,000
Account prefix K bits	4

1. **Total Nodes in Network:** For simulation, we consider a network consisting of 10,000 nodes. These nodes are essential for the implementation and evaluation of the sharding protocol.

2. **Number of network sharding:** We divide the blockchain network into 16 different shards for our experimentation. Each shard operates independently, allowing for parallel processing of transactions.

3. **Leader election probability:** In our experiments, the probability of a node being elected as a leader was set at 0.0001. The leader node plays a crucial role in packaging and publishing the final blocks.

4. **The total number of transactions:** For simulations, we generated and processed a total of 10,000 transactions. This transaction volume allowed us to analyze the protocol's efficiency and throughput.

5. **Account prefix K bits:** The sharding scheme employed a prefix-based approach to divide transactions among different shards. Each account's address was considered, and the first 4 bits of the address were used for sharding.

During the conducted experiments, we utilized Python as our programming language to implement the sharding protocol and conduct the necessary simulations and analyses. The outcomes derived from these experiments were fundamental in evaluating the efficiency and effectiveness of the proposed sharding mechanism.

Throughout this thesis, we thoroughly analyze the efficacy of the introduced sharding protocol by investigating transaction volume, the number of sharding instances, and transaction processing time under diverse scenarios. Fig 5.1 depicts the correlation between transaction volume and processing time under a constant sharding configuration. As observed in the graph, when the sharding number is set to 1 and transactions are not partitioned into blocks, the transaction volume progressively increases, leading to notable transaction processing delays. This bottleneck is caused by the P2P network architecture. On the other hand, correctly sharding transactions can significantly reduce processing time overhead. The experimental findings indicate that once a specific threshold is surpassed, adjusting the number of shards has minimal impact on the time required for transaction processing.

In Fig 5.2, we can observe the correlation between the number of shards and the processing time of transactions at different transaction volumes. As illustrated, the transaction processing time experiences a notable decline as the number of shards grows. According to eq (4.1), as the number of shards, represented by *"m"*, expands, the transaction volume also grows linearly, with the growth rate being equivalent to the number of shards. Similarly, Fig. 5.1 demonstrates that while maintaining a constant time to perform a transaction, the number of shards' expansion results in a rapid increase in transaction volume on each shard. Consequently, this leads to a substantial rise in the entire number of transactions on the blockchain network *(M)* in comparison to *mM1*.

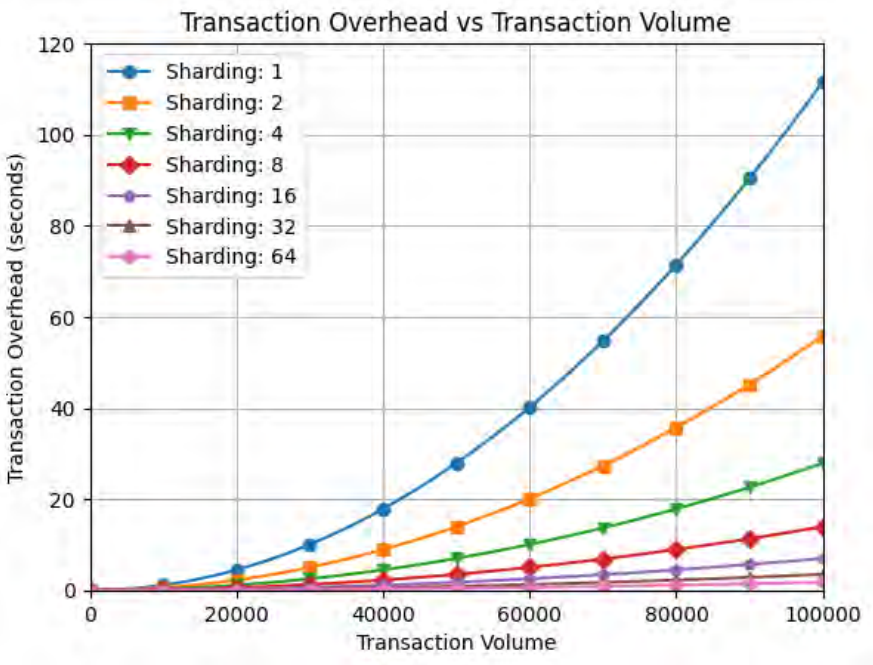

Figure 5.1: Transaction Volume and Transaction Processing Overhead

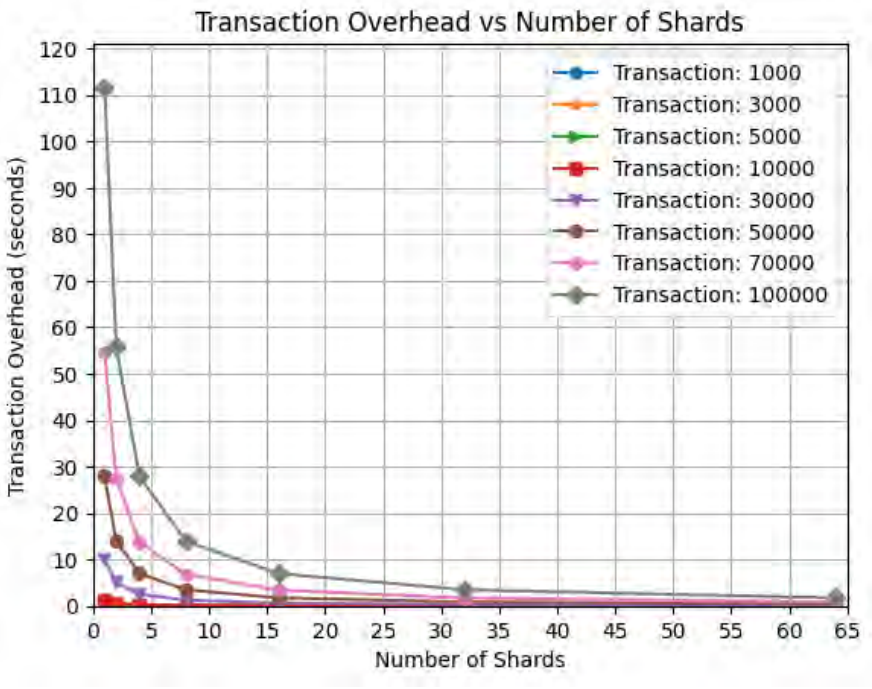

Figure 5.2: Number of Sharding and Transaction Processing Time

This observation aligns with eq. 3.3, which indicates the exponential decrease in transaction processing time with an increasing number of shards. However, it's essential to note that after reaching a specific number of shards, the transaction processing overhead stabilizes and shows only slight variations while remaining relatively constant.

Fig 5.3 demonstrates the correlation between the number of shards and transaction processing overhead for various trading volumes when the entire network consists of more than 100,000 nodes and processes over 10,000 transactions. As the size of the blockchain node network increases significantly, more shards can be created to accommodate higher transaction volumes, without incurring a proportional increase in transaction processing time overhead. This means that a larger network can efficiently handle a substantial volume of transactions without compromising the processing speed.

From the data in Fig 5.3, it becomes evident that the optimal transaction processing time overhead hovers around 5 seconds. This indicates that with the appropriate number of shards, the blockchain network can strike a

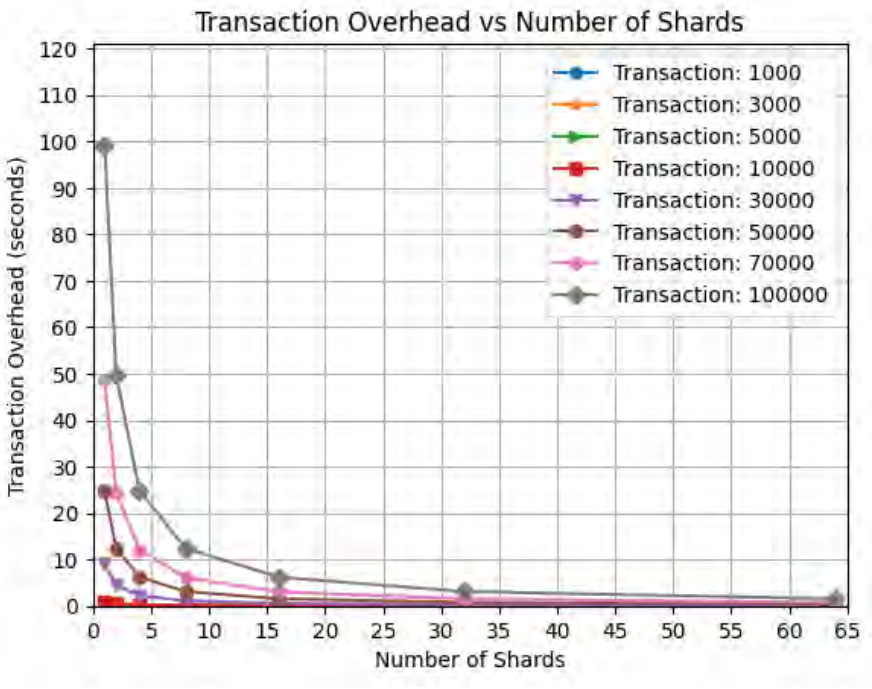

Figure 5.3: Number of Shards and Transaction Processing Overhead

balance between transaction volume and processing time, ensuring efficient and timely processing of transactions even at a larger scale.

5.1 Improvement

Table 5.2: Experimental Parameters

Name	**Value**
Nodes in the entire network	10,000
Network sharding	32
Probability of leader election	0.0001
Number of transactions	10,000
Account prefix K bits	4

In the presented evaluation, we aimed to improve the performance of the Gradingshard protocol by doubling the network sharding to 32 (Table 5.2).

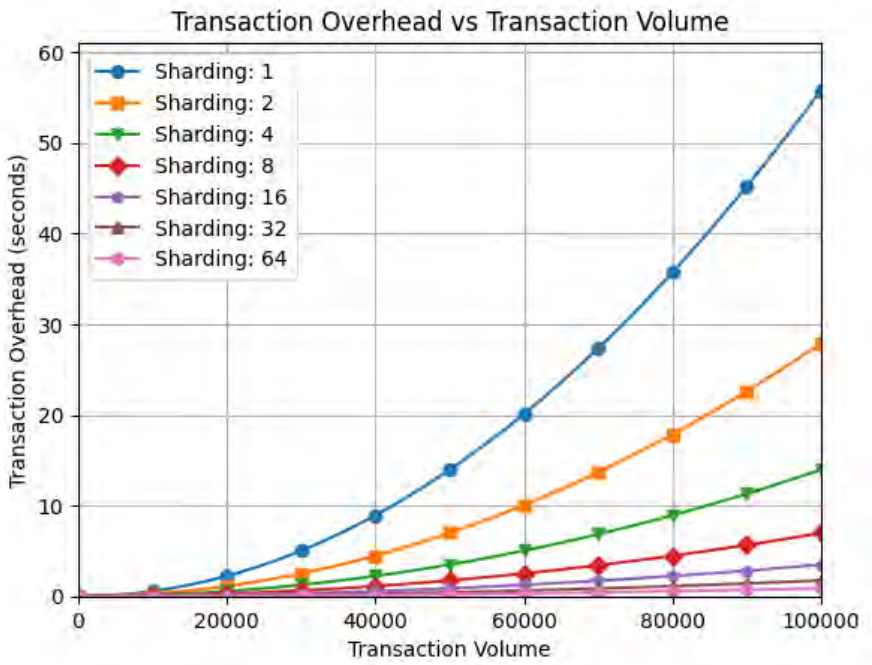

Figure 5.4: Transaction Volume and Transaction Processing Overhead

The results revealed a substantial enhancement, as the improved graph exhibited nearly half the time (55 seconds) for the transaction overhead compared to the transaction volume graph (Fig 5.4). This significant reduction in transaction processing time demonstrates the protocol's scalability and efficiency, making it a promising solution for handling higher transaction volumes in large-scale blockchain networks. The experiments underscore the potential of the Gradingshard protocol to meet the demands of future blockchain applications with increased throughput requirements.

In the second graph, Fig 5.5, we explore the correlation between the number of shards and the processing time of transactions at different transaction volumes. By doubling the network sharding to 32, we achieved a remarkable improvement in performance. As depicted in the graph, the transaction overhead is nearly halved compared to the previous results obtained with 16 shards. This significant reduction in transaction processing time indicates a substantial increase in efficiency and scalability when using a larger number of shards. The enhanced graph provides valuable insights into the Gradingshard protocol's ability to handle higher transaction volumes and

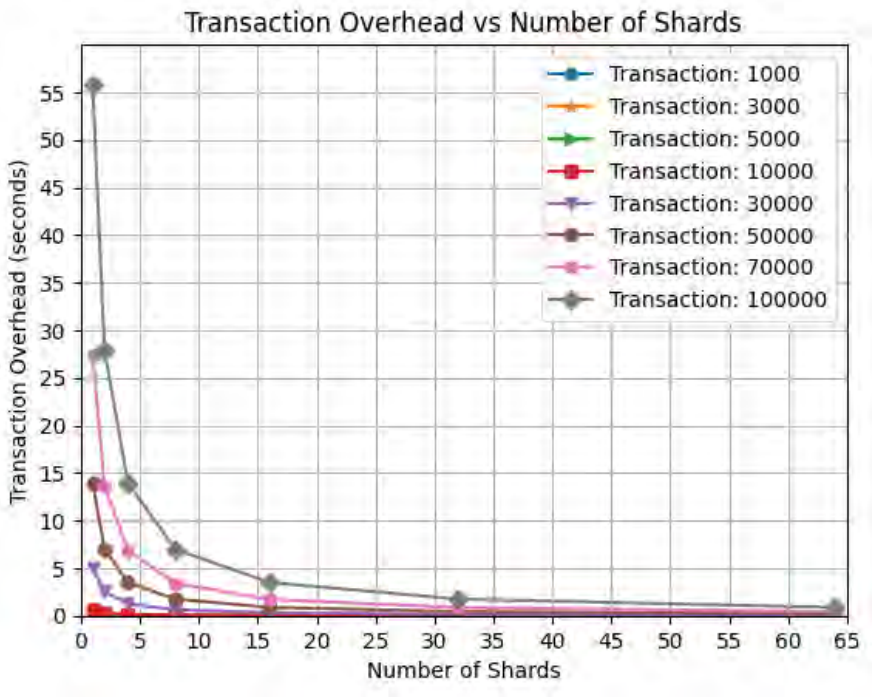

Figure 5.5: Number of Shards and Transaction Processing Overhead

highlights its potential to effectively address the throughput challenges faced by large-scale blockchain networks

In Fig 5.6, we present the improved relationship between the number of shards and transaction processing overhead at different trading volumes, considering a blockchain network with over 100,000 nodes and processing over 10,000 transactions. By doubling the network sharding to 32, we achieved a significant enhancement in performance. The transaction processing time has been notably reduced, taking only 22.5 seconds compared to the previous 45 seconds. This improvement, nearly half of the previous processing time, showcases the remarkable scalability and efficiency of the Grading-shard protocol. The enhanced graph demonstrates the protocol's capability to handle higher transaction volumes with improved time efficiency, making it a promising solution to address the scalability challenges in large-scale blockchain networks.

Doubling the network sharding in blockchain technology, specifically increasing it from 16 to 32, represents a significant scaling effort with potential

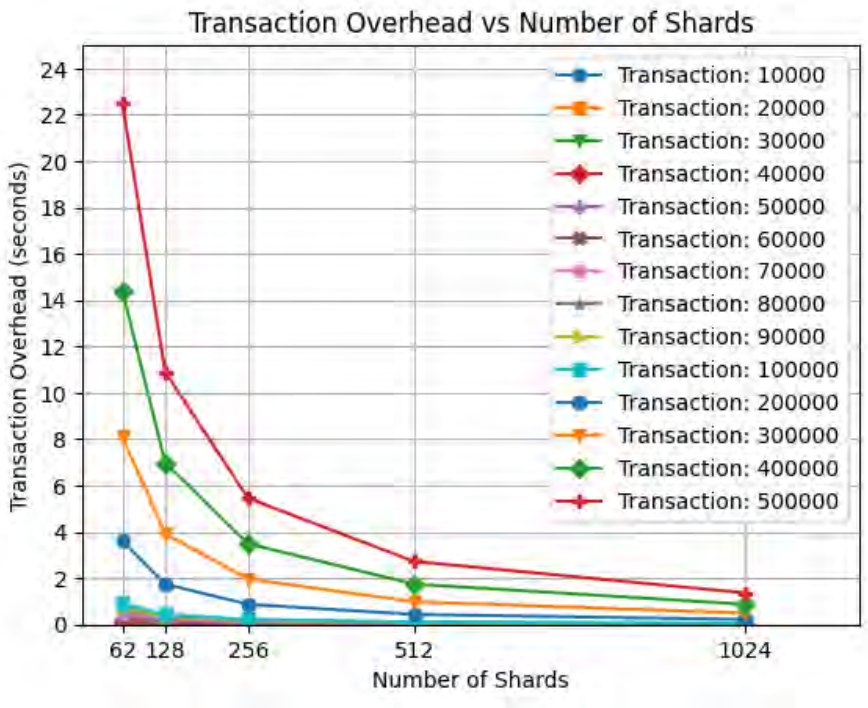

Figure 5.6: Number of Shards and Transaction Processing Overhead

implications for both the system's complexity and associated hardware costs. Sharding is a method employed to enhance the scalability of blockchain networks by partitioning the network into smaller, more manageable segments. While the increase from 16 to 32 shards can theoretically improve throughput and processing capacity, it also introduces a higher level of intricacy into the overall network architecture. Managing a larger number of shards demands more sophisticated coordination mechanisms, potentially making the system more intricate to design, implement, and maintain. Moreover, the expansion of the sharding infrastructure may require additional hardware resources to support the heightened computational demands, thereby increasing overall hardware costs. Striking a balance between scalability and complexity is crucial in the evolution of blockchain technology, as it involves navigating the trade-offs between enhanced performance and the practical challenges associated with managing a more intricate and resource-intensive network.

Chapter 6

Conclusion

Blockchain technology has gained significant attention as a decentralized distributed ledger system with the potential to revolutionize various industries. However, its current scalability issues, especially concerning storage space and transaction throughput, pose substantial challenges to its widespread adoption. The efficiency bottleneck primarily lies in transaction throughput, making it a crucial area of research for improving blockchain performance. Researchers have focused on consensus protocols and algorithms to enhance the efficiency of blockchains, but the existing research on sharding, a promising solution for scalability, remains limited. Therefore, the low throughput performance of blockchain technology remains a pressing concern that demands effective solutions.

In response to this challenge, this thesis proposes the utilization of sharding technology to boost blockchain transaction throughput. Sharding, which involves the parallel processing of transactions within the blockchain, has gained increasing attention among researchers due to its theoretical and practical significance. Through the subdivision of the blockchain network into smaller shards and simultaneous processing of transactions, sharding has the potential to significantly improve the overall throughput of the system.

In order to tackle the issue of low transaction throughput in conventional blockchains, this research introduces a novel sharding protocol called "GradingShard," which combines both network sharding and transaction sharding. The GradingShard protocol aims to overcome the limitations imposed by cross-shard communication and improve the scalability and efficiency of blockchain networks.

To evaluate the effectiveness of the proposed GradingShard protocol,

extensive experiments were conducted using Python as the programming language. These experiments tested the enhanced blockchain structure, including network sharding and transaction sharding functionalities. The results demonstrated a positive correlation between the number of shards in a blockchain network and the transaction volume being processed. As per the theoretical analysis, this correlation follows a linear growth pattern. However, the experimental Python results, which considered factors like network delay and other variables, revealed even more promising outcomes, surpassing the linear growth ratio. These Python-based experiments underscored the significant potential of GradingShard in enhancing blockchain transaction throughput.

In conclusion, the proposed GradingShard protocol offers a promising solution to address the low transaction throughput problem in blockchain technology. By leveraging sharding technology and conducting experiments with Python, this research provides valuable contributions to enhancing the efficiency and scalability of blockchain systems, paving the way for widespread adoption across various industries.

Chapter 7

Future Work

Embarking on future work within the domain of network sharding in blockchain technology, particularly within the context of the Grading shard protocol, necessitates a comprehensive examination of the associated complexities and hardware cost implications. The adoption of a dual-sharding approach, encompassing both transaction sharding and network sharding, within the Grading shard protocol lays the foundation for a scalable and parallelized blockchain system. However, as we envision doubling the network sharding from 16 to 32, it becomes imperative to delve into the increased complexity that such an expansion introduces.

The heightened intricacy arises from the need to design and implement more sophisticated coordination mechanisms to manage the larger number of shards effectively. Future research should address the challenges related to optimizing the interplay between transaction and network sharding, ensuring seamless communication and coordination across the expanded network structure. Moreover, the exploration of potential hardware cost escalations is paramount. The doubling of network sharding may demand additional computational resources, necessitating an in-depth analysis of efficient resource allocation strategies to mitigate potential increases in hardware costs. Striking a balance between scalability, complexity management, and cost-effectiveness is a critical aspect of future work in this dynamic field, paving the way for advancements in blockchain technology that are both scalable, sustainable, and economically viable.

Bibliography

[1] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PloS one*, vol. 11, no. 10, p. e0163477, 2016.

[2] A. Manimuthu, R. Sreedharan V., R. G., and D. Marwaha, "A literature review on bitcoin: Transformation of crypto currency into a global phenomenon," *IEEE Engineering Management Review*, vol. 47, no. 1, pp. 28–35, 2019.

[3] R. Grinberg, "Bitcoin: An innovative alternative digital currency," *Hastings Sci. & Tech. LJ*, vol. 4, p. 159, 2012.

[4] C. Gupta and A. Mahajan, "Evaluation of proof-of-work consensus algorithm for blockchain networks," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7, 2020.

[5] B. Sriman, S. Ganesh Kumar, and P. Shamili, "Blockchain technology: Consensus protocol proof of work and proof of stake," in *Intelligent Computing and Applications: Proceedings of ICICA 2019*, pp. 395–406, Springer, 2021.

[6] G. Blossey, J. Eisenhardt, and G. Hahn, "Blockchain technology in supply chain management: An application perspective," 2019.

[7] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, 2018.

[8] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–3, 2016.

[9] F. . Hjálmarsson, G. K. Hreiarsson, M. Hamdaqa, and G. Hjálmtỳsson, "Blockchain-based e-voting system," in *2018 IEEE 11th international conference on cloud computing (CLOUD)*, pp. 983–986, IEEE, 2018.

[10] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges," *Journal of network and computer applications*, vol. 177, p. 102857, 2021.

[11] Y. Chen and C. Bellavitis, "Decentralized finance: Blockchain technology and the quest for an open financial system," *Stevens Institute of Technology School of Business Research Paper*, 2019.

[12] P. Treleaven, R. Gendal Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.

[13] A. Manimuthu, G. Rejikumar, D. Marwaha, *et al.*, "A literature review on bitcoin: Transformation of crypto currency into a global phenomenon," *IEEE Engineering Management Review*, vol. 47, no. 1, pp. 28–35, 2019.

[14] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, vol. 4, no. 2, p. 15, 2008.

[15] C. L. Read, "The genesis block," in *The Bitcoin Dilemma: Weighing the Economic and Environmental Costs and Benefits*, pp. 29–36, Springer, 2022.

[16] W. Metcalfe *et al.*, "Ethereum, smart contracts, dapps," *Blockchain and Crypt Currency*, vol. 77, 2020.

[17] Y. Wang, W. Wang, Y. Zeng, and T. Yang, "Gradingshard: A new sharding protocol to improve blockchain throughput," *Peer-to-Peer Networking and Applications*, pp. 1–13, 2023.

[18] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," *Applied Sciences*, vol. 11, no. 20, p. 9372, 2021.

[19] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and scalability," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 122–128, 2018.

[20] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Network*, vol. 33, no. 5, pp. 166–173, 2019.

[21] R. Wang, K. Ye, and C.-Z. Xu, "Performance benchmarking and optimization for blockchain systems: A survey," in *Blockchain–ICBC 2019: Second International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings 2*, pp. 171–185, Springer, 2019.

[22] L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais, "Sok: Off the chain transactions.," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 360, 2019.

[23] A. O. Bada, A. Damianou, C. M. Angelopoulos, and V. Katos, "Towards a green blockchain: A review of consensus mechanisms and their energy consumption," in *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 503–511, 2021.

[24] B. K. Chauhan and D. B. Patel, "A systematic review of blockchain technology to find current scalability issues and solutions," in *Proceedings of Second Doctoral Symposium on Computational Intelligence: DoSCI 2021*, pp. 15–29, Springer, 2022.

[25] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *2018 IEEE symposium on security and privacy (SP)*, pp. 583–598, IEEE, 2018.

[26] J. Wang and H. Wang, "Monoxide: Scale out blockchains with asynchronous consensus zones," in *16th USENIX symposium on networked systems design and implementation (NSDI 19)*, pp. 95–112, 2019.

[27] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access*, vol. 8, pp. 14155–14181, 2020.

[28] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: Scaling blockchain via full sharding," in *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pp. 931–948, 2018.

[29] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 17–30, 2016.

[30] J. Yun, Y. Goh, and J.-M. Chung, "Trust-based shard distribution scheme for fault-tolerant shard blockchain networks," *IEEE Access*, vol. 7, pp. 135164–135175, 2019.

[31] D. Yang, C. Long, H. Xu, and S. Peng, "A review on scalability of blockchain," in *Proceedings of the 2020 the 2nd International Conference on Blockchain Technology*, pp. 1–6, 2020.

[32] J. Stark, "Making sense of ethereum's layer 2 scaling solutions: State channels, plasma, and truebit," *Medium. com*, 2018.

[33] C. Sguanci, R. Spatafora, and A. M. Vergani, "Layer 2 blockchain scaling: A survey," *arXiv preprint arXiv:2107.10881*, 2021.

[34] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K.-K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *Journal of Network and Computer Applications*, vol. 149, p. 102471, 2020.

[35] S. Kim, Y. Kwon, and S. Cho, "A survey of scalability solutions on blockchain," in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 1204–1207, IEEE, 2018.

[36] S. S. Hazari and Q. H. Mahmoud, "A parallel proof of work to improve transaction speed and scalability in blockchain systems," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0916–0921, 2019.

[37] G. Wang, Z. J. Shi, M. Nixon, and S. Han, "Sok: Sharding on blockchain," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, pp. 41–61, 2019.

[38] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn, and G. Danezis, "Chainspace: A sharded smart contracts platform," *arXiv preprint arXiv:1708.03778*, 2017.

[39] Y. Gao, S. Kawai, and H. Nobuhara, "Scalable blockchain protocol based on proof of stake and sharding," *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol. 23, no. 5, pp. 856–863, 2019.

[40] A. Durand, E. Anceaume, and R. Ludinard, "Stakecube: Combining sharding and proof-of-stake to build fork-free secure permissionless distributed ledgers," in *Networked Systems: 7th International Conference, NETYS 2019, Marrakech, Morocco, June 19–21, 2019, Revised Selected Papers 7*, pp. 148–165, Springer, 2019.

[41] D. R. Lee, Y. Jang, and H. Kim, "Poster: A proof-of-stake (pos) blockchain protocol using fair and dynamic sharding management," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2553–2555, 2019.

[42] N. Jiang, F. Bai, L. Huang, Z. An, and T. Shen, "Reputation-driven dynamic node consensus and reliability sharding model in iot blockchain," *Algorithms*, vol. 15, no. 2, p. 28, 2022.

[43] L. Vishwakarma and D. Das, "Blocktree: a nonlinear structured, scalable and distributed ledger scheme for processing digital transactions," *Cluster Computing*, vol. 24, no. 4, pp. 3751–3765, 2021.

[44] F. Hashim, K. Shuaib, and F. Sallabi, "Medshard: Electronic health record sharing using blockchain sharding," *Sustainability*, vol. 13, no. 11, p. 5889, 2021.

[45] A. Begum, A. Tareq, M. Sultana, M. Sohel, T. Rahman, and A. Sarwar, "Blockchain attacks analysis and a model to solve double spending attack," *International Journal of Machine Learning and Computing*, vol. 10, no. 2, pp. 352–357, 2020.

[46] M. Yu, S. Sahraei, S. Li, S. Avestimehr, S. Kannan, and P. Viswanath, "Coded merkle tree: Solving data availability attacks in blockchains," in *International Conference on Financial Cryptography and Data Security*, pp. 114–134, Springer, 2020.