International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

# A Scalable Sharding Approach Leveraging Blockchain: State-of-the-art

**Kritika Pandey[1]· Udai Shanker[2]**

[1,2]Dept. of Computer Sc. & Engg. Madan Mohan Malaviya University of Technology Gorakhpur, India,
[1]2022028003@mmmut.ac.in, [2]uscs@mmmut.ac.in

**Abstract**
Blockchain technology (BT) has significantly expanded its applications across diverse sectors, leveraging its key attributes of anonymity, decentralization, and resistance to tampering within peer-to-peer (P2P) networks. It has made inroads into smart manufacturing and intelligent Medicare systems, along with the development of smart cities, showcasing its potential to revolutionize traditional industry practices by enhancing data security and efficiency. Additionally, it finds its application in digital identity management, secure voting systems, and supply chain tracking. The future holds promise as blockchain continues to disrupt various sectors with its innovative capabilities. While traditional blockchain technology has grappled with scalability issues, limiting its use in high-throughput and low-latency environments, efforts are underway to overcome these limitations. Sharding, a method that involves partitioning the network to reduce duplication of computations, storage, and communication overhead, is a key enabler of horizontal scalability as the network expands. A consensus technique is employed to attach the freshly generated block to the end of the current chain.

**Keywords:** Blockchain, Sharding, scalability, consensus algorithm, permissioned, permissionless.

## 1 Introduction

Blockchain technology (BT) has become widely accepted since the 2008 debut of Bitcoin, a popular peer-to-peer payment system [1]. BT is widely acknowledged for promoting decentralization, transparency, and tamper resistance. The benefits have led to the extensive implementation of BT across nearly all sectors, particularly in artificial intelligence, IoT, supply chain management, social welfare, and administrative functions [2-4]. Blockchain, which consists of seven layers in its technological architecture, as depicted in Figure 1, is being regarded as a disruptive technology following cloud computing, IoT, and Big Data. Governments, financial institutions, and tech businesses worldwide are deeply concerned about this issue, given the disruptive nature of blockchain technology.

However, the main concern of industry has always been the scalability of blockchain, raising questions about whether widespread commercial use of technology will actually occur. To be more specific, Bitcoin [1] can only process 7 transactions in a second, whereas Ethereum [5] can process 15 transactions in a second. In contrast, EOS [6] can process hundreds of transactions per second. Number of transactions that can be handled quickly, or throughput, is much less than the real requirements for transaction processing. Enhancing transaction throughput poses considerable risk to embrace BT. However, with the development of solutions like sharding and off-chain scaling, the scalability issue is being addressed. "Visa's impressive capability to handle 1,700 transactions per second emphasizes the critical necessity of addressing the scalability issue in BT. Subsequently it demands immediate attention to unleash the limitless potential of blockchain.

Prior research has often overlooked a clear exposition of scalability. Buterin, a co-founder of Ethereum, who initially articulated what is now renowned as the scalability trilemma [7]. He posited that a trade-off among the three fundamental attributes of BT, decentralization, security, and scalability—is inescapable.

The fundamental and inherent characteristic of BT is its decentralization; moreover, security represents a necessary feature. Concurrently, the primary challenge it faces is scalability. Only one of the following factors can be present at a time: scalability, security, or decentralization. Trade-offs are practically inevitable.

Enhancing scalability within a blockchain-based framework presents a significant challenge without undermining the principles of security and decentralization. Academic literature has presented various concepts to tackle the issue of scalability. In our analysis, we categorize these solutions into three groups based on the blockchain technical logic architecture: Layer 0 solutions (such as BDN [8] and bloXroute [9]), Layer 1 solutions (such as Segregated Witness [10], DAG [11–13], sharding [14–17], and consensus [18–20]), and Layer 2 solutions (such as state channels [21], side chains [22], cross chains [23], and off-chain computation [24]. Layer 0 solutions aim to enhance scalability through modifications in the blockchain's fundamental data transmission protocol. These adjustments aim towards improvement of underlying framework of blockchain network, thus allowing for more efficient processing and handling of transactions. Layer 1 solutions focus on increasing scalability through modifications to the foundational aspects of the blockchain protocol. These modifications include adjustments to block data structures, consensus mechanisms, and incentive models. Layer 2 findings strive to enhance scalability within application layer through implementation of off-chain techniques.

However, these suggested fixes are unable to significantly improve performance without compromising security, decentralization, or both. A particularly notable solution to the issue of scalability without compromising decentralization and security is sharding. Sharding involves division of network into numerous groups, known as shards, each of which is responsible for processing transactions concurrently. This method significantly enhances network's capacity to process transactions efficiently and securely [25]. This study focuses on sharding, acknowledged as a very valid technique for addressing scalability challenges in BT.

In recent studies [10, 25–28], sharding strategies based on blockchain have been presented for security. Blockchain sharding has been increasingly recognized in academic studies on scalability issues of blockchain [29–34], which previously concentrated solely on vertical scaling and minimizing overhead. However, none of them can systematically outline the limitations and features of the sharding systems currently in use, as well as the challenges and emerging trends.

## 2 OUR CONTRIBUTION

Our approach to introducing sharding mechanisms is more systematic and thorough compared to previous surveys and studies. Below, we highlight our key contributions.

1. This research provides the first comprehensive examination of blockchain scaling methods, encompassing a wide range of scalability solutions and technical logic architectures. Among these methods, sharding is identified as a scalable approach that preserves both security and decentralization.
2. Various investigations have been done on shard-based blockchain methodologies, delivering comprehensive analysis and providing insights into the inherent characteristics and constraints of these frameworks. Among the aspects and limitations discussed are the security vulnerabilities associated with intra-shard consensus mechanisms and the complications arising from ensuring atomicity in cross-shard transactions.
3. In conclusion, we identify the limitations present in existing sharding methods and offer recommendations for the future development of robust and dependable sharding systems.

## 3 Related Work

As part of our research, we have rigorously examined and assessed previous studies on the scalability of blockchain technology [30, 33, 35–37]. Prior research has primarily focused on enhancing scalability issues of blockchain and expanding the blockchain network efficiently. Additionally, various academics

are introducing new concepts to enhance the scalability of blockchains. Several of these solutions encompass multichain architecture, scalable consensus mechanisms, Directed Acyclic Graphs (DAG), block expansion, and Segregated Witness.

The exploration of scalability in BT has been a critical area of study. Numerous publications, as referenced [31-38], have substantially contributed to understanding various methodologies to address this issue. Despite the comprehensive insights provided by these studies into potential remedies for scalability concerns, they collectively overlook the concept of sharding. Sharding has recently emerged as a prominent approach for improving the scalability of blockchain systems. This gap in literature signifies the need for further exploration into sharding as an effective and feasible approach to achieving a scalable blockchain architecture. Before the development of BT, it was already being used in traditional databases, mainly for optimizing large-scale commercial databases. The concept entails fragmenting the database data into several smaller units, which are subsequently allocated across different servers for storage purposes. This strategy enhances data management and accessibility. Sharding is regarded as the most efficient technique for horizontally scaling blockchain systems. Thus, numerous scholars have proposed their own sharding mechanisms. The evaluation and introduction of sharding are unclear, with each study only examining and assessing one or two sharding processes. Bez et al. [40] emphasize isolating data and reaching consensus as vital for increasing horizontal scalability in their proposed three-dimensional architecture. The consensus layer in [3] is separated from the ledger topology layer, which is improper in a sharding system due to the significance of intra-consensus. This provides only a vague introduction to Ethereum 2.0.

Reference [43] proposes a Nakamoto-based sharding approach (Monoxide), which is now considered outdated. Nakamoto-based and BFT-based sharding mechanisms are not comprehensively compared in Ref. [15, 44].

To our knowledge, our contribution exceeds all existing surveys by thoroughly examining the fundamental concept of diverse sharding systems and providing a thorough comparison for users based on our views.

## 4 Preliminaries

### SHARDING APPROACH

Sharding is a widely used technique in distributed databases and cloud infrastructures that was first introduced in [45]. Sharding technology has been successfully integrated with both permissioned and permissionless blockchains, following pioneering suggestions [14, 46], and implementing sharding technology in blockchain involves dividing the network into several subnetworks. This approach enhances the system's efficiency and scalability.

The idea behind sharding technology originates from traditional centralized databases. In this approach, a database is systematically partitioned into distinct, individual shards to manage data more efficiently. In BT, sharding signifies the method of dividing the network into multiple segments, each referred to as a shard. This approach is adopted to enhance the scalability and efficiency of the blockchain by distributing the computational and storage workload across different shards. As illustrated in Figure 1, the framework includes primary layers of sharding techniques.

***1.*** **State Sharding:** State sharding in BT involves dividing a network's global state into multiple portions or shards. State sharding significantly reduces storage requirements in blockchain networks since each node maintains only a segment of the full ledger, as opposed to transaction sharding. This approach allows for more scalability and efficiency in data management.

***2.*** **Network Sharding:** The most essential technique for sharding is known as network sharding. Within a blockchain network, nodes are distributed across multiple shards in a random manner. Node allocation methods typically incorporate both functional and non-functional approaches to distribution.

***3.*** **Transaction Sharding:** In transaction sharding, transactions are segmented into multiple shards, with each shard maintaining a full copy of blockchain. This allows for concurrent processing of

transactions on each node, thereby enhancing the system's efficiency by distributing the workload. Cross-chain communication must be enhanced to guarantee the accurate synchronization of transactions using the same inputs but distributed across different shards.

## 5 Systematic Survey on Sharding

In this Part, we analyze the latest sharding strategies and their role in improving blockchain scalability. Our discussion encompasses various dimensions of sharding and scaling methodologies within the blockchain technology framework.

The introduction of sharding presents new challenges, most notably in the security of intra-shard consensus protocol, ensuring the atomicity of cross-shard transactions, and overall enhancements needed for reconfiguration, latency, and storage management.

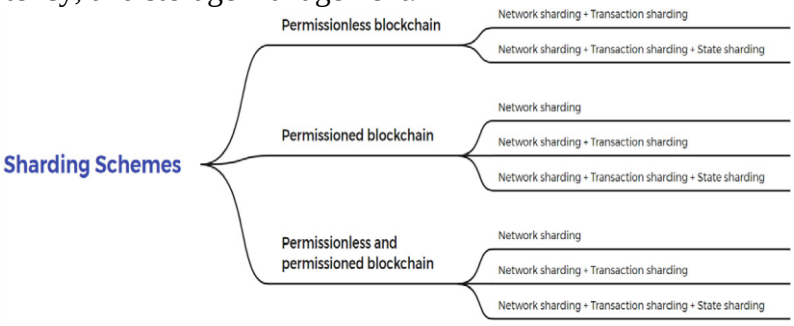


Figure 1. Sharding Schemes

## 6 Sharding Evaluation Criteria

Evaluation criteria are essential for comparing and identifying the pros and cons of various blockchain sharding techniques. By conducting a comprehensive and rigorous examination of various sharding techniques according to specific evaluation criteria, we can confidently identify outstanding issues and future research directions. In this section, we focus on addressing research issues mentioned in Section 5 and present a set of evaluation criteria, such as scalability, applicability, and reliability, to assess the effectiveness of the sharding techniques discussed in Section 6. Figure 2 illustrates the taxonomy of the evaluation criteria.

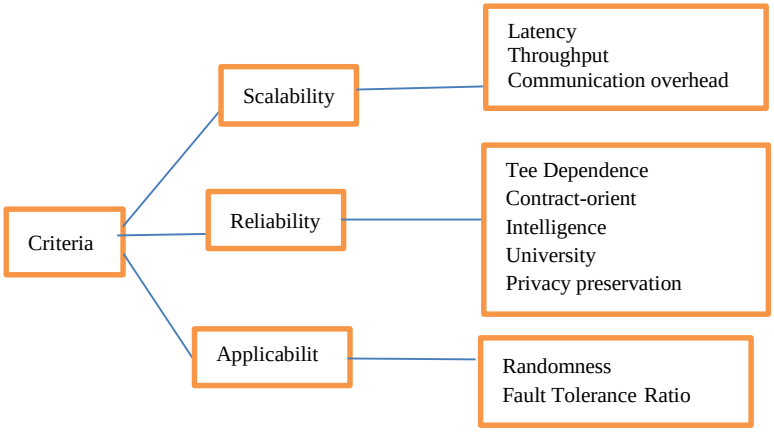


Figure 2 : Sharding Evaluation Criteria

**A. Scalability:** A scalable sharding technique implies that it maintains its efficiency and functionality even with an increasing workload. Characterized by a high volume of transactions, a scalable blockchain

system is capable of maintaining its operations as usual or even enhancing its performance. Three primary criteria are essential for assessing the scalability of a sharding scheme in academic contexts- communication overhead, latency, and throughput.

1. **Latency:** The duration elapsed from the moment a transaction is submitted to the blockchain to the point when a block containing that transaction is validated is referred to as the transaction's latency. In real-time applications, minimizing latency is imperative due to its direct influence on processing speed and response time, which are critical factors for performance.
2. **Throughput:** When evaluating the scalability of a sharding scheme, throughput stands as a crucial measure of effectiveness. The capacity of a blockchain network to efficiently process a substantial volume of transactions is contingent upon its throughput. This capability, in turn, diminishes the total operational expenditures associated with the network's management.
3. **Communication Overhead:** The communication overhead of a sharding method is essential, as it entails the transfer of data between shards to authenticate both intra-shard and cross-shard transactions. It has a direct impact on the efficiency of blockchain consensus mechanisms and consequently influences the system's throughput.

**B. Applicability:** An effective sharding method is one that is versatile and applicable across various contexts. We suggest employing the following standards to evaluate whether a sharding strategy is appropriate.

1. **TEE Dependency:** Sharding schemes that rely on Trusted Execution Environments (TEEs) are referred to as TEE-dependent [49, 50]. This limitation on the versatility of a sharding method stems from its reliance on Trusted Execution Environments (TEEs), which in turn makes it dependent on the underlying hardware and software platforms [51]. Secure computations, access control enforcement, and data encryption are just a few of the features that TEEs offer [52]. The utilization of TEEs might constrain the overall flexibility and portability of the sharding technique, even though they enhance security and contribute to flexibility.
2. **Contract-Oriented:** When employing a contract-oriented sharding strategy, it signifies that the strategy is designed to be compatible with smart contracts. It facilitates the appropriate execution, in line with prior agreements, of a series of conditional digital commitments [53, 54]. Smart contracts can be utilized to enforce various regulations, including transaction fees, transaction size limitations, and data privacy standards. Additionally, they can automatically verify transactions [55].
3. **Intelligence:** To adapt to a variety of application scenarios, a sharding system requires extensive reconfiguration of its settings. The intelligence of a sharding scheme is characterized by its ability to autonomously optimize settings through a learning mechanism, such as machine learning [56-58].
4. **Privacy Preservation:** Due to the inherent transparency of blockchain technology, it is possible for the general public to access user identities and the data stored within. Preserving privacy is essential to prevent the disclosure of confidential user information [59, 60]. In a sharding scheme, it is imperative to employ effective techniques to thwart the aggregation of adversarial nodes across shards, thereby safeguarding user data and identity privacy.

### 6.1 Permissioned blockchains using Sharding

This section explores the current permissioned blockchain sharding schemes.

**A. Network sharding schemes**

**Blockchain architecture that is scalable and uses spontaneous sharding to transfer value:** Value-transfer ledgers (VTL) constitute the foundational element of Ren et al.'s [47] sharding technology for value transfer, ensuring both decentralization and reliability within an asynchronous network configuration. The system has the ability to accept 33% Byzantine nodes due to the use of PBFT within each shard for consensus. Furthermore, as the number of network nodes expands, both throughput and cross-shard communication overhead show a linear increase. The PBFT consensus mechanism is exclusively applicable to blockchains that operate within a permissionless framework.

**B. Transaction sharding scheme and Network sharding scheme:** In a permissioned blockchain network, the implemented strategies leverage both transaction and network sharding.

**RSCoin**: The RSCoin dual-layered cryptocurrency system was developed by Danezis and Meiklejohn [48] to assist banks in managing the trading of digital currency within an asynchronous network. After several time intervals have passed, the central bank releases an updated global report. When a specific shard size is maintained, overhead associated with intra-shard communication exhibits a quadratic growth. However, latency remains unaffected, and system throughput sees a linear enhancement in response to an increase in total number of nodes.

**C. Network sharding, transaction sharding, and state sharding:** These strategies leverage the comprehensive capabilities of the permissioned blockchain network, including network sharding, transaction sharding, and state sharding, to improve efficiency and security.

**1. RChain:** Tree-based sharding architecture, as presented by Greg et al. [49] in RChain, utilizes account-based transactions in an asynchronous network. The CasperCBC consensus mechanism, which belongs to the "Correct-by-Construction" set of protocols, guarantees system consistency and can accept 33% Byzantine nodes. In a distributed ledger environment, the overhead associated with cross-shard communication escalates quadratically as the number of shards expands. Concurrently, throughput of system enhances linearly with an increase in the count of nodes.

**2. Chainspace:** A cryptocurrency system capable of efficiently managing account-based transactions in an asynchronous environment was introduced by Mustafa et al. [50]. Chainspace introduces the Sharded Byzantine Atomic Commit (S-BAC), a distributed consistency protocol designed to shard generic smart contract transactions across a broad array of Byzantine nodes, thereby ensuring their synchronized operation to enhance security. This method aims to achieve consensus among participating nodes, enhancing the system's overall integrity and reliability in processing transactions. It maintains a consistent latency and demonstrates linear scalability in throughput as the number of shards increases while being capable tolerating up to 33% of faulty nodes. Communication overhead inside the shard experiences a quadratic increase as the shard size increases. Conversely, the communication overhead among different shards is determined by a formula that is proportional to the square of both the number of shards and the size of each shard. Manage Contracts allows users to create smart contracts that prioritize their privacy.

**3. Channels:** The state-sharding approach, which features low computational overhead within a synchronous system employing UTXO-based transactions, was proposed by Androulaki et al. [51]. This approach is called "Channel". The method utilizes a Single-Channel Transaction Protocol (SCTP) to authenticate transactions within shards, in conjunction with Atomic Cross-Channel (ACC) consensus to ensure a uniform global state. The overhead associated with cross-shard communication directly proportional to the square of both the shard size and the number of shards, whereas the overhead for intra-shard communication exhibits a quadratic increase as a function of the shard size.

**4.** **SharPer:** In asynchronous network environments featuring crash-only fault-tolerant (CFT) nodes, Amiri et al. [52] introduced an effective sharding strategy [53]. The system has the potential to accept 50% Byzantine nodes, leveraging PBFT and MultiPaxos consensus mechanisms for validation of account-based transactions. As the quantity of nodes within a network augments, there is a linear escalation in both latency and throughput observed. The complexity of both intra-shard and cross-shard communications escalates at a quadratic rate in relation to the number of shards and is directly proportional to size of per shard.

**5.** **Meepo:** Zheng et al. [54] introduced Meepo, A system has been designed to enhance the efficiency of cross-shard account-based transactions. This innovation combines an effective cross-shard validation protocol with a sophisticated method for aggregating and sending data. Proof of Authority (PoA) is validation selection protocol utilized by Meepo. As the number of nodes in a network increases, the proportional rise in both its throughput and latency.

### 6.2 Sharding schemes in permissionless blockchains

In permissionless BT, paper initiates its discourse by presenting a comprehensive summary and analysis of the prevailing sharding strategies. This analysis includes a comprehensive review of systems that integrate multiple sharding approaches to optimize scalability and performance.
The permissionless blockchain network utilizes the following methods to implement both transaction and network sharding.

**1.** **ELASTICO:** Sharding technology was originally introduced by Luu et al. [55] within the context of a partially synchronous network architecture for permissionless blockchains. All of the validators in ELASTICO have comparable computational and network capabilities. Utilizing a proof-of-work solution (PoW) [56] alongside an identity-establishment mechanism (PoW-ID), this approach initially employs network sharding to segment nodes into multiple committees, known as shards, for enhanced efficiency and security. Each committee, which maintains a Failure to Respond (FTR) rate of 33%, is required to achieve consensus on a chunk that includes UTXO transactions. This process is guided by the principles of intra-shard BFT consensus [57]. To create final chunk and achieve persistent global state, a directory committee convenes to collect chunks from every individual committee and confirm their impression.

**2.** **Zilliqa:** The innovative cryptocurrency platform Zilliqa[58] facilitates asynchronous, permissionless blockchains by employing a scalable collaborative signature technique known as CoSi. The PBFT consensus mechanism, designed to accept 33% of the network's Byzantine nodes, represents practical approach to Byzantine fault tolerance based on EC-Schnorr signatures and is utilized to authenticate account-based transactions [59,60,61]. The throughput of the system increases in a linear manner as the total amount of shards increases. As the shape of the shard expands, its communication overhead escalates quadratically. Zilliqa utilizes formally verifiable Scilla language to facilitate contract-oriented programming. It supports sharding, enabling the execution of complex and large-scale arithmetic operations in parallel. One such mechanism is employed by Zilliqa, which introduces a two-phase method for node allocation. This methodology distinguishes itself through an innovative strategy, merging address-based solutions with the classical PoW mechanism to efficiently allocate nodes across its network.

**3.** **Poster:** The blockchain protocol proposed by Lee et al. [62] is a dynamic shard management system based on PoS. It operates in an asynchronous network. This approach effectively solves the problem of unequal allocation of nodes and transactions within sharding, resulting in a significant improvement in the distribution mechanism. A poster represents a flexible and dependable protocol that

operates on the basis of account transactions. To accommodate up to a 33% tolerance for Byzantine nodes, the approval process for the shard block implements the Byzantine Fault Tolerance (BFT) intra-shard consensus mechanism. As the size of a shard increases, the cost associated with intra-shard communication increases quadratically. This concept is applicable to other sharding schemes as well, providing support for universality.

4. **Optchain:** Hguyen et al. [63] presented an approach named optchain aimed at reducing the overhead associated with cross-shard transactions. This method is both lightweight and capable of real-time transaction allocation, leveraging the UTXO model for efficiency in partially synchronous networks. As the total amount of shards increases, the latency of system exhibits log-linear increase, whereas the throughput demonstrates a logarithmic increase. The purpose of the Transactions as Nodes (TaN) network is to reduce the overhead associated with cross-shard transactions. It achieves this by conceptualizing both nodes and transactions within the framework of an online DAG.

5. **Repchain:** Huang et al. proposed the first double-chain system that incorporates incentives through sharding, which they named Repchain [64,65]. In RepChain, each node is randomly allocated to an individual shard, as depicted in Figure 7. Subsequently, at the commencement of every shard's operation, a leader for that shard is selected. In the realm of distributed ledger technology, the Intra-shard Collective Signing Byzantine Fault Tolerance (CSBFT) consensus, along with the Atomix consensus mechanism [66,67], plays a pivotal role. Specifically, each shard employs a reputation chain, which is constructed on the basis of transaction records. This design aims to provide resilience against up to 33% Byzantine nodes, thereby enhancing the system's reliability and integrity. Subsequently, the construction of a transaction chain is facilitated through the implementation of the Raft consensus protocol [68,69], further solidifying the network's consensus mechanism. Each shard then finalizes the reputation and transaction chains within a state block. Repchain can perform state synchronization and updates at the end of every epoch, ensuring a consistent global state through the use of state blocks produced by shards. The size of a shard directly influences its latency and throughput. While the cross-shard communication overhead rises linearly with the number of shards, the intra-shard communication overhead is connected with the square of the shard size.

### A. Network sharding, transaction sharding and state sharding

#### Sharding in Open Blockchains with Smart Contracts

1. **RapidChain:** Based on the Cuckoo rule [70], Zamani et al. [66] introduced RapidChain, a blockchain architecture that features sharding and is resilient to slowly adaptive Byzantine adversaries. The system utilized a 33% Fault Tolerant Rapid Shard Consensus (RSC) mechanism to validate transactions within a shard. Integrating RapidChain effectively reduced the constant time complexity that escalates as the network size increases. This improvement was particularly notable in a synchronous network environment that employs Unspent Transaction Outputs (UTXO)-based transactions. As the total number of nodes increases, the throughput exhibits a linear growth pattern. As the network size expands, the overhead associated with intra-shard communication increases quadratically. Simultaneously, the complexity of the overhead for cross-shard communication adheres to **O (m^2 + m log n).** In RapidChain, every shard executes a Distributed Random Generation (DRG) protocol internally. This protocol generates an unbiased random value, which is then used to construct a reference committee.

2. **Monoxide:** To address the challenge of substantial cross-shard communication overhead within asynchronous networks, Wang et al. developed Monoxide, a concurrent multichain system [71]. Network nodes and transactions are initially allocated among numerous asynchronous consensus zones, commonly

referred to as shards, as depicted in Figure 8. To validate transactions within a single shard, the system employed a Proof of Work (PoW) consensus mechanism, which featured a 50% Fault Tolerance Rate (FTR). In the context of cross-shard communication, the Eventual Atomicity consensus algorithm plays a crucial role. It verifies operations and validates transactions on an account-by-account basis across different zones, thereby ensuring atomicity. This mechanism is critical in maintaining consistency and integrity within distributed ledger environments. Moreover, they proposed "Chu-ko nu Mining," a novel network sharding strategy enabling miners to validate several blocks across various zones simultaneously. The latency in Monoxide exhibits a logarithmic increase, whereas the throughput demonstrates a linear growth as the number of shards escalates. While its cross-shard communication exhibits a complexity of **O(m+n)**, the overhead for intra-shard communication directly correlates with the quantity of shards involved.

3. **SSChain:** In a sharding architecture, the reconfiguration process effectively mitigates the threat posed by slowly adaptive adversaries. Nevertheless, this protective measure incurs substantial costs in terms of both bandwidth and time. In this blockchain architecture designed for UTXO transactions, nodes have the capability to join one or more shards by leveraging the Proof of Work (PoW) Identification method, ensuring resilience against Byzantine failures. In the SSChain architecture, there exists a direct correlation between the size of a shard and the system's throughput, as well as between the number of shards and the system's latency. The intra-shard communication overhead, however, escalates quadratically with the increase in shard size. For the purpose of validating intra-shard transactions and maintaining the integrity of the global state, even in the presence of up to 50% byzantine nodes, the system employs a Proof-of-Work consensus mechanism

4. **Ethereum 2.0:** Buterin's proposal, Ethereum 2.0, builds upon Ethereum 1.0 and introduces 64 shard chains in addition to a Beacon Chain, to enhance scalability and security. Each shard within the Beacon Chain is overseen by a dedicated validator committee, responsible for supervising the activities of all validators within that shard. For intra-shard consensus, each shard employs a hybrid Proof of Stake (PoS) consensus mechanism known as Casper the Friendly Finality Gadget (Casper FFG). This method is designed to be robust against up to 33% Byzantine nodes. Given that Ethereum 2.0 adheres to the RD criteria, its protocol mandates that committees are rotated and chosen through a multi-stage random number generation (RNG) process [72], enhanced by the verifiable delay function known as RANDAO [73]. In terms of communication overhead within distributed systems, there correlation between the number of shards and the overhead associated with intra-shard communication. However, it is observed that the overhead related to cross-shard communication distinctly correlates with the square of the size of the shards. Ethereum 2.0, in its current form, is limited to facilitating account-based transactions within individual shards.

5. **Pyramid:** The Pyramid blockchain system, enabling overlapping shards and allowing nodes to reside in multiple shards, represents the inaugural stacked sharding system equipped with a layered sharding consensus, as introduced by Hong et al. [70]. Pyramid incorporates a unique hierarchical sharding consensus that allows partial shards to store the overall state of the blockchain. It validates and commits cross-shard transactions in a single round. Pyramid utilizes a unique hierarchical sharding consensus allowing partial shards to store the overall blockchain state and validating and committing cross-shard transactions in a single round. Cross-shard communication exhibits a computational complexity of **O(m^2 + n^2).** Nevertheless, it is observed that both the latency and the throughput of the network improve linearly as the number of nodes within the network expands.

**6. Free2Shard:** A reputation-based dynamic self-allocation policy for synchronous networks called Free2Shard was first presented in scholarly work by Rana et al. [74]. The structured architecture permits the employment of diverse consensus mechanisms across different shards. In the network, while the throughput escalates logarithmically and the cross-shard communication overhead grows linearly as the number of nodes increases, the latency consistently remains unchanged. The dynamic self-allocation (DSA) mechanism implemented by Free2Shard randomly assigns nodes.

### 6.3 Sharding schemes in permissionless blockchains and permissioned blockchains

In this section, we critically review current sharding schemes implemented within both permissionless and permissioned blockchain environments.

#### A. Network sharding, transaction sharding and state sharding

The following schemes utilize network sharding, transaction sharding, and state sharding in both permissionless and permissioned blockchain networks.

**1. Space-aware Representations using State Sharding:** Mizrahi and Rottenstreich [75] introduced a traffic-aware sharding system, which significantly mitigates cross-shard communication overhead. This innovative approach is underpinned by the utilization of a memory-efficient mapping technique, ensuring that system components are regularly monitored and effectively combined to optimize performance. This method represents a notable advancement in reducing the bottlenecks typically associated with cross-shard communication. The technology is versatile as it can be used with both permissioned and permissionless blockchain systems without being tied to a specific consensus mechanism.

**2. Ostraka:** In the context of the non-democratic environment of Ostraka, Manuskin et al. [76] proposed a scaling node architecture that facilitates the participation of a single node in multiple shards simultaneously. As number of shards increases, system's latency grows logarithmically, while its throughput increases linearly. In systems characterized by the unequal distribution of voting power, this mechanism can be effectively integrated with additional consensus methodologies.

**3. OmniLedger:** The OmniLedger, a scale-out distributed ledger technology, was introduced by Kokoris Kogias et al. [77], drawing upon the foundational concepts of ELASTICO [79]. OmniLedger, composed of various shard chains along with an identity chain, enhances security and efficiency while simultaneously maintaining the global state. OmniLedger is deployed using a partially synchronous network, which facilitates the validation of UTXO-based transactions through Atomix intra-shard consensus and ByzCoinX. The network tolerates the presence of Byzantine nodes, allowing for up to 25% of the nodes to behave in a Byzantine manner. The latency is directly proportional to the number of nodes. As the number of shards increases, both its throughput and cross-shard communication cost increase in a linear manner. Additionally, it is observed that with the enlargement in shard size, the internal communication overhead within a shard exhibits a logarithmic increment. By integrating RandHound [80] with a Verifiable Random Function (VRF)-based leader election algorithm [81].

#### B. Network sharding and transaction sharding

The aforementioned strategies utilize network sharding and transaction sharding within both permissionless and permissioned blockchain networks, catering to various academic and practical applications.

1. **DQNSB:** In their study, Yun et al. [82] presented a sharding technique known as DQNSB, which leverages the deep Q-learning algorithm to dynamically optimize sharding configurations. In this provided strategy, intra-shard transactions are validated through the application of the 33% Fault Tolerance Ratio (FTR) PBFT consensus mechanism. In scenarios involving fewer than 1000 nodes, throughput experiences a linear increase. Conversely, in situations with more than 1000 nodes, the throughput stabilizes and maintains a constant level. Moreover, the latency remains unaffected, however, as size of the shard expands, intra-shard communication overhead experiences a quadratic increase. DQNSB generates the optimal throughput configuration for large-scale IoT blockchain systems [83], employing a deep reinforcement learning (DRL) approach alongside analytical latency equations [84].
2. **Fleetchain:** Liu et al. [85] suggested the implementation of Fleetchain to decrease the overhead associated with cross-shard communication. The framework introduces a Responsive Sharding Transaction Processing (RSTP) for cross-shard consensus, alongside a Fast Byzantine Fault Tolerance (FBFT) mechanism for intra-shard consensus. These are built upon a reliable (t, u)-multi-signature protocol and a Two-Phase Commitment (2PC) protocol, enhancing the system's security and efficiency [86]. It is capable of processing UTXO-based transactions within a partially synchronous network and can tolerate up to 33% Byzantine nodes. The complexity of cross-shard communication overhead is precisely represented by O(n^2 + m), while the communication overhead within a shard is definitively proportional to the square of the shard size.
3. **Polyshard:** Polyshard [87] employs a Lagrangian-encoded computing framework within its polynomial coding sharding system. Noisy polynomial interpolation techniques, including Reed-Solomon decoding, are employed by Polyshard to inhibit malicious nodes from producing erroneous results [88]. This perspective significantly enhances storage performance, as latency of Polyshard displays a linear increase correlated with running time, shard size, and number of shards. The throughput capacity of the network is linearly influenced by the total number of nodes within it. This approach allows for the computation and storage of encoded transactions, aiming to minimize the use of storage space.

## 7 Open Issues in Blockchain Sharding

In this part, we considered several open issues, including communication overhead, synchronization, automation, universality, intelligence, and privacy protection. These issues are identified based on the detailed research and analysis previously presented.

***1.*** **Lack of automatic sharding:** The outcomes of the present research fail to provide adequate support for the efficient and secure implementation of automatic sharding. The foundational premise of smart contracts was to obviate the necessity for intermediary parties. Accordingly, an agreement can be executed autonomously via smart contracts, thereby negating the need for any intermediaries and eliminating associated delays. This facilitates the accurate implementation of sophisticated digital contracts in accordance with the stipulations of prior agreements. Nevertheless, current frameworks merely employ smart contracts for the purpose of executing transactions; they fail to autonomously allocate nodes or manage transactions with efficiency, stability, and security throughout the sharding process.

***2.*** **Security deficiency**: Every sharding method has inherent drawbacks. Specifically, network sharding introduces security concerns due to its practice of randomly partitioning nodes, failing to account for their heterogeneity, such as differences in trustworthiness [89]. Moreover, there is a notable discrepancy in the computational power of nodes within individual shards, attributed to the lack of

consideration for the unique capabilities of each node. This discrepancy may adversely affect the overall efficiency of the blockchain system, particularly if leads to a disproportionate allocation of workloads among shards during the processing of transactions. To address the double-spending problem, implementing cross-shard validation in transaction sharding leads to increased communication overhead. Moreover, because different shards process transactions in varying sequences, this approach can lead to conflicts and inconsistencies within the blockchain system. It is essential to ensure that nodes do not collude in order to manipulate the blockchain. State sharding increases the need for more storage space as it requires maintaining a comprehensive backup of the blockchain's global state. Moreover, a centralized backup solution creates a single point of failure, introducing vulnerability that elevates the risk of security breaches. Attackers could exploit specific shards to execute attacks such as double-spending or other malicious activities.

***3.*** **Low Communication Overhead:** Cross-shard transactions often lead to a significant decrease in throughput during the consensus process, mainly due to the high communication overhead involved. When a transaction involves multiple shards, such as transferring assets between users on different shards, it requires inter-shard communication to reach consensus. Communication between different shards can greatly slow down the process, creating a major bottleneck. Traditional blockchain consensus mechanisms, such as PoW and certain PoS variants, tend to become inefficient when implemented across multiple shards. This inefficiency primarily appears as increased latency and reduced throughput, creating challenges in achieving consensus across shards.

***4.*** **Ignorance of Sharding Synchronization:** The current research rarely addresses sharding synchronization, especially in the context of asynchronous networks. While current sharding strategies increase blockchain network capacity by processing transactions concurrently, not all of them consider that a blockchain system typically operates in an unsynchronized network. In an asynchronous network, nodes with varying perspectives of the network's overall state may struggle to develop an efficient sharding technique. This significantly impacts the efficiency of reaching a consensus and makes achieving atomicity challenging.

***5.*** **Limited Cross-Shard Functionality:** Current sharding schemes have not achieved sufficient ubiquity. These methods are preferred because of their capacity for various applications, suggesting strong applicability and low maintenance costs. Nonetheless, the development of sharding demands capacities beyond what existing sharding systems currently deliver. One disadvantage of majority of recent research is that it is scenario-specific, which restricts its generalizability.

***6.*** **Limited Adaptability:** Current sharding techniques often lack the ability to adapt to changing network conditions or transaction patterns, requiring manual intervention to optimize performance or prevent bottlenecks. After reviewing and analyzing the data, it's clear that the way transactions and nodes are assigned has a big impact on sharding efficiency. Unfortunately, most research relies on predetermined configurations to initiate sharding in various scenarios, which means that adaptive sharding performance cannot be effectively guaranteed. The current optimization methods for assigning nodes and transactions have limitations. They focus only on local optimization and overlook global optimization. Therefore, creating a sharding solution that can adapt to various scenarios and ensure optimal performance remains a challenging and unsolved issue [90].

***7.*** **Lack of privacy protection**: Currently, there is minimal research on effective methods for preserving privacy within sharding frameworks. The details of transactions recorded on the blockchain, including user IDs, are easily accessible to the public. Moreover, the identity of an individual initiating a

smart contract can be exposed during the process of its invocation. Many modern sharding systems often overlook the importance of privacy protection. Neither approach is considered suitable for widespread adoption due to their inherent limitations and implementation challenges. Therefore, more comprehensive research on privacy-preserving sharding in literature is needed.

## 8 Future directions in sharding

1. **Smart contracts for sharding automation:** Sharding systems with smart contract capabilities improve automation and security. However, enhancing efficiency remains a significant challenge that requires further scholarly inquiry. The implementation of smart contracts, which facilitate automation and obviate the requirement for an authorized intermediary, underscores the importance of integrating smart contract support within sharding systems. Pertaining to cross-shard communication, further research is necessary to optimize the use of smart contracts and reduce unnecessary communication overhead.
2. **High-performance sharding with minimal communication overhead:** In the future, research should focus on developing effective sharding techniques that minimize communication overhead. The performance of blockchain systems is significantly compromised by cross-shard transactions with existing consensus mechanisms, primarily due to the substantial communication costs incurred during the consensus determination process. To efficiently minimize cross-shard communication overhead while still upholding other quality attributes, it is essential to explore new consensus methodologies. Additionally, it is crucial to explore a consensus mechanism that is efficient in communication to reduce the cost of block consensus communications. To minimize data transmission within and between shards, it is recommended to explore advanced encoding and compression techniques.
3. **Investigation of the universal sharding system:** There is widespread anticipation in the academic community that upcoming research will concentrate on developing universal sharding systems suitable for deployment in a wide range of conditions. The appeal of such systems lies in their broad applicability and low maintenance demands, making them easy to adopt in practical applications. A significant challenge for scholars is to ensure that a sharded blockchain system maintains high transactional throughput. Achieving high performance remains a crucial factor for the adoption of any universal sharding solution.
4. **Maximizing security and trust by intelligently using sharding:** Sharding in blockchain technology should be dynamic, considering the changing network topology and transaction volume. There is a need for adaptive sharding mechanisms capable of intelligently adjusting to ensure optimal blockchain performance across various applications and contexts. Integration of security and trust evaluation processes within the sharding infrastructure is essential to optimize shard trustworthiness and security effectively. Consequently, a significant research question arises: How can blockchain performance be improved in various scenarios by implementing intelligent sharding solutions, while also addressing security and trust considerations in a nuanced manner?
5. **Effective maintenance of privacy:** Research on privacy protection in sharded blockchain systems is crucial, as few existing methods successfully accomplish this objective. Crafting a lightweight strategy that doesn't negatively impact the system's performance poses a significant challenge. It is crucial that the implementation of privacy measures does not significantly degrade the throughput and latency of a sharded blockchain system.
6. **Ongoing investigation of various sharding techniques:** The objectives of enhancing sharding technology research ought to concentrate on mitigating the shortcomings of current approaches. It is

imperative for researchers to delve into advanced algorithms for network sharding that segregate nodes by their heterogeneity—namely, their performance capabilities and reliability. This strategy guarantees that every shard is composed of reliable nodes possessing adequate capacity, and it strives to optimize workload distribution to the highest degree practicable. Efficiently designed cross-shard communication protocols can significantly enhance transaction-sharding efforts by averting the risk of double spending. This enhancement significantly reduces the overhead associated with processing transactions across various shards, thereby minimizing the occurrence of inconsistencies and conflicts within the blockchain infrastructure [91]. Furthermore, to bolster the security of sharding techniques and thwart node collusion, further investigation is imperative [92]. Research on state sharding should prioritize decreasing storage expenses and devising innovative security strategies to protect against targeted shard attacks and double-spending scenarios. It is essential to explore secure backup techniques that require low storage load or are lightweight. Overall, additional research should concentrate on enhancing the efficiency, security, and scalability of sharding approaches in order for them to be effectively implemented in both established and developing blockchain systems.

## 9 Conclusion

The study elucidates the logical architecture of BT and examines the associated trilemma. It articulates the concept of sharding, emphasizing its critical role in achieving scalable blockchain design. Furthermore, it categorizes the current state-of-the-art sharding mechanisms, encompassing intra-shard consensus protocols, cross-shard transaction atomicity, and a range of general enhancements. We provide a detailed analysis that includes precise calculations and unique insights into the characteristics and limitations of the examined sharding processes. This study evaluates these processes from multiple dimensions, offering a comprehensive comparison and assessment.

## Reference

1. S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” Decentralized Business Review, Article ID 21260, 2008.
2. O. Novo, “Blockchain meets IoT: an architecture for scalable access management in IoT,” IEEE Internet of things Journal, vol. 5, no. 2, pp. 1184–1195, 2018.
3. R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, “Integrated blockchain and edge computing systems: a survey, some research issues and challenges,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1508–1532, 2019.
4. X. Wang, X. Zha, W. Ni et al., “Survey on blockchain for Internet of things,” Computer Communications, vol. 136, pp. 10–29, 2019. [30] Xie H, Fei S, Yan Z, Xiao Y.
5. G. Wood, “Ethereum: a secure decentralised generalised transaction ledger,” Ethereum Project YELLOW paper, vol. 151, no. 2014, pp. 1–32, 2014.
6. B. Xu, D. Luthra, Z. Cole, and N. Blakely, “Eos: an architectural, performance, and economic analysis,” vol. 11, p. 2019, 2018, https://whiteblock.io/wp-content/uploads/ 2019/07/eostest-report.pdf.
7. A. Hafid, A. S. Hafid, and M. Samih, “Scaling blockchains: a comprehensive survey,” IEEE Access, vol. 8, pp. 125244–125262, 2020.
8. A. Kuzmanovic, “Net neutrality,” Communications of the ACM, vol. 62, no. 5, pp. 50–55, 2019.
9. U. Klarman, S. Basu, A. Kuzmanovic, and E. G. Sirer, “Bloxroute: a scalable trustless blockchain distribution network whitepaper,” IEEE Internet of things Journal, 2018.

10. A. Singh, R. M. Parizi, M. Han, A. Dehghantanha, H. Karimipour, and K.-K. R. Choo, "Public blockchains scalability: an examination of sharding and segregated witness," Blockchain Cybersecurity, Trust and Privacy. Advances in Information Security, Springer, vol. 79, Cham, Switzerland,2020.
11. S. Popov, "The tangle," White paper, vol. 1, no. 3, 2018.
12. A. Churyumov and Byteball, "A decentralized system for storage and transfer of value," 2016, https://byteball.org/ Byteball.pdf.
13. Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "Spectre: a fast and scalable cryptocurrency protocol," IACR Cryptol. ePrint Arch.vol. 2016, no. 1159, 2016.
14. 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, Vienna, Austria, October 2016.
15. G. Wang, Z. J. Shi, M. Nixon, S. Han, and Sok, "Sharding on blockchain," in Proceedings of the 1st ACM Conference on Advances in Financial Technologies, pp. 41–61, Zurich, Switzerland, October 2019.
16. 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.
17. G.Yu, X.Wang, K.Yu, W.Ni, J.A.Zhang, and R.Liu, Scaling out Blockchains with Sharding: An Extensive Survey, Institution of Engineering and Technology (IET), London, UK, 2020.
18. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in Proceedings of the 2017 IEEE International Congress on Big Data (Big Data Congress), pp. 557–564, IEEE, Honolulu, HI, USA, June 2017.
19. D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 2567–2572, IEEE, Banff, Canada, October 2017.
20. S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain-based vanet," Information Sciences, vol. 545, pp. 170–187, 2021.
21. S. Dziembowski, S. Faust, and K. Hostakova, "General state channel networks," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 949–966, Toronto, Canada, October 2018.
22. X. Xu, I. Weber, M. Staples et al., "A taxonomy of blockchain based systems for architecture design," in Proceedings of the 2017 IEEE International Conference on Software Architecture (ICSA), pp. 243–252, IEEE, Gothenburg, Sweden, April 2017.
23. M. Herlihy, "Atomic cross-chain swaps," in Proceedings of the 2018ACMSymposiumonPrinciplesofDistributedComputing, pp. 245–254, Egham, UK, July 2018.
24. J. Poon and T. Dryja, "The Bitcoin lightning network: scalable off-chain instant payments," 2016, https://lightning.network/ lightning-network-paper.pdf.
25. S. S. Chow, Z. Lai, C. Liu, E. Lo, and Y. Zhao, "Sharding Blockchain," in Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), p. 1665, IEEE, Halifax, Canada, July-August 2018.

26. H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards scaling blockchain systems via sharding," in Proceedings of the 2019 International Conference on Management of Data, pp. 123–140, Amsterdam Netherlands, June-July 2019.
27. M. Zamani, M. Movahedi, M. Raykova, and Rapidchain, "Scaling blockchain via full sharding," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 931–948, Toronto, Canada, October 2018.
28. E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: a secure, scale-out, decentralized ledger via sharding," in Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), pp. 583–598, IEEE, San Francisco, CA, USA, May 2018.
29. W. Gao, W. G. Hatcher, and W. Yu, "A Survey of Blockchain: Techniques, Applications, and Challenges," in Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1–11, IEEE, Hangzhou, China, July-August 2018.
30. S. Kim, Y. Kwon, and S. Cho, "A Survey of Scalability Solutions on Blockchain," in Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC), pp. 1204–1207, IEEE, Jeju Island, South Korea, October 2018.
31. L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in Proceedings of the 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1–5, IEEE, Coimbatore, India, January 2017.
32. Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.
33. 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.
34. W. Wang, D. T. Hoang, P. Hu et al., "A survey on consensus mechanisms and mining strategy management in blockchain networks," IEEE Access, vol. 7, pp. 22328–22370, 2019.
35. A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and Scalability," in Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 122–128, IEEE, Lisbon, Portugal, July 2018.
36. P. W. Eklund and R. Beck, "Factors that impact blockchain scalability," in Proceedings of the 11th International Conference on Management of Digital Ecosystems, pp. 126–133, Limassol, Cyprus, November 2019.
37. Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to the scalability of blockchain: a survey," IEEE Access, vol. 8, pp. 16440–16455, 2020.
38. L. Kan, Y. Wei, A. H. Muhammad, W. Siyuan, L. C. Gao, and H. Kai, "A multiple blockchains architecture on inter blockchain communication," in Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 139–145, IEEE, Lisbon, Portugal, July 2018.
39. W. Yang, S. Garg, A. Raza, D. Herbert, and B. Kang, "Blockchain: trends and future," in Proceedings of the Pacific Rim Knowledge Acquisition Workshop, pp. 201–210, Springer, Nanjing, China, August 2018.
40. M. Bez, G. Fornari, and T. Vardanega, "The Scalability Challenge of Ethereum: An Initial Quantitative Analysis," in Proceedings of the 2019 IEEE International Conference on Service-Oriented System Engineering (Sose), pp. 167–176, IEEE, San Francisco East Bay, CA, USA, April 2019.

41. M. H. Manshaei, M. Jadliwala, A. Maiti, and M. Fooladgar, "A game-theoretic analysis of shard-based permissionless blockchains," IEEE Access, vol. 6, pp. 78100–78112, 2018.
42. Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1432–1465, 2020.
43. J. Wang and H. Wang, "Monoxide: scale-out blockchains with asynchronous consensus zones," in Proceedings of the 16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI}19), pp. 95–112, Boston, MA, USA, February 2019.
44. P. Singhal and S. Masih, "Meta-analysis of methods for scaling blockchain technology for automotive uses," 2019, https:// arxiv.org/abs/1907.02602.
45. J. C. Corbett, P. Hochschild, W. Hsieh et al., "Spanner," ACM Transactions on Computer Systems, vol. 31, no. 3, pp. 1–22, 2013.
46. G. Danezis and S. Meiklejohn, "Centrally banked cryptocurrencies," 2015, https://arxiv.org/abs/1505.06895.
47. Ren Z, Cong K, Aerts T, de Jonge B, Morais A, Erkin Z. A scale-out blockchain for value transfer with spontaneous sharding. In: 2018 Crypto Valley conference on blockchain technology. 2018, p. 1–10.
48. Danezis G, Meiklejohn S. Centrally banked cryptocurrencies. 2015, p. 934–50, arXiv preprint arXiv:1505.06895.
49. Greg M, Ed E, Kenny R, Evan J, Aleksandr B, Ian B. RChain Whitepaper 2021 (ver0.1). 2017, https://rchain.coop/whitepaper.html.
50. Al-Bassam M, Sonnino A, Bano S, Hrycyszyn D, Danezis G. Chainspace: A sharded smart contracts platform. 2017, arXiv preprint arXiv:1708.03778.
51. Androulaki E, Cachin C, Caro AD, Kokoris-Kogias E. Channels: Horizontal scaling and confidentiality on permissioned blockchains. In: European symposium on research in computer security. 2018, p. 111–31.
52. Amiri M, Agrawal D, El Abbadi A. Sharper: Sharding permissioned blockchains over network clusters. In: Proceedings of the 2021 international conference on management of data. 2021, p. 76–88.
53. How the consensus protocol impacts blockchain throughput. 2022, https: //www.nec.com/en/global/insights/CONFERENCE/2020022520/index.html.
54. Zheng P, Xu Q, Zheng Z, Zhou Z, Yan Y, Zhang H. Meepo: Sharded consortium blockchain. In: 2021 IEEE 37th international conference on data engineering. 2021, p. 1847–52.
55. Luu L, Narayanan V, Zheng C, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016, p. 17–30.
56. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Bus Rev 2008;21260.
57. Lamport L, Shostak R, Pease M. The Byzantine general's problem. In: Concurrency: The works of Leslie lamport. 2019, p. 203–26.
58. Dong X, Prateek S, Christel Q, Jia Y, Max K. The zilliqa project: A secure, scalable blockchain platform. 2020.
59. Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery. ACM Trans Comput Syst (TOCS) 2002; 20:398–461.

60. Castro M, Liskov B, et al. Practical byzantine fault tolerance. In: OsDI. 99, 1999, p. 173–86.
61. De Angelis S, Aniello L, Baldoni R, Lombardi F, Margheri A, Sassone V. PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. 2018.
62. Lee DR, Jang Y, Kim H. 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. 2019, p. 2553–5.
63. Nguyen LN, Nguyen TD, Dinh TN, Thai MT. Optchain: optimal transactions placement for scalable blockchain sharding. In: 2019 IEEE 39th international conference on distributed computing systems. 2019, p. 525–35.
64. Huang C, Wang Z, Chen H, Hu Q, Zhang Q, Wang W, et al. Repchain: A reputation-based secure, fast, and high incentive blockchain system via sharding. IEEE Internet Things J 2020; 8:4291–304.
65. Han R, Yan Z, Liang X, Yang LT. How can incentive mechanisms and blockchain benefit with each other? a survey. ACM Comput Surv (CSUR) 2022;55(7):1–38
66. Zamani M, Movahedi M, Raykova M. Rapidchain: Scaling blockchain via full sharding. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security. 2018, p. 931–48.
67. Kogias EK, Jovanovic P, Gailly N, Khoffi I, Gasser L, Ford B. Enhancing bitcoin security and performance with strong consistency via collective signing. In: 25th usenix security symposium. 2016, p. 279–96.
68. Huang D, Ma X, Zhang S. Performance analysis of the raft consensus algorithm for private blockchains. IEEE Trans Syst Man Cybern 2019; 50:172–81.
69. Howard H. ARC: analysis of raft consensus. Tech. rep, University of Cambridge, Computer Laboratory; 2014.
70. Sen S, Freedman MJ. Commensal cuckoo: Secure group partitioning for large-scale services. ACM SIGOPS Oper Syst Rev 2012; 46:33–9.
71. Wang J, Wang H. Monoxide: Scale out blockchains with asynchronous consensus zones. In: 16th USENIX symposium on networked systems design and implementation. 2019, p. 95–112.
72. L'Ecuyer P. Random number generation. In: Handbook of computational statistics. 2012, p. 35–71.
73. What is randomness. 2022, https://eth2.incessant.ink/book/06__building blocks/02__randomness.html.
74. Hong Z, Guo S, Li P, Chen W. Pyramid: A layered sharding blockchain system. In: IEEE INFOCOM 2021-IEEE conference on computer communications. 2021, p. 1–10.
75. Mizrahi A, Rottenstreich O. State sharding with space-aware repre sentations. In: 2020 IEEE international conference on blockchain and cryptocurrency. ICBC, 2020, p. 1–9.
76. Manuskin A, Mirkin M, Eyal I. Ostraka: Secure blockchain scaling by node sharding. In: 2020 IEEE European symposium on security and privacy workshops. 2020, p. 397–406.
77. Kokoris-Kogias E, Jovanovic P, Gasser L, Gailly N, Syta E, Ford B. Om niledger: A secure, scale-out, decentralized ledger via sharding. In: 2018 IEEE symposium on security and privacy. 2018, p. 583–98.
78. Luu L, Narayanan V, Zheng C, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016, p. 17–30.

79. Syta E, Jovanovic P, Kogias EK, Gailly N, Gasser L, Khoffi I, et al. Scalable bias-resistant distributed randomness. In: IEEE symposium on security and privacy. 2017, p. 444–60.
80. Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N. Algorand: Scaling byzantine agreements for cryptocurrencies. In: Proceedings of the 26th symposium on operating systems principles. 2017, p. 51–68.
81. Zheng P, Xu Q, Zheng Z, Zhou Z, Yan Y, Zhang H. Meepo: Sharded consortium blockchain. In: 2021 IEEE 37th international conference on data engineering. 2021, p. 1847–52.
82. Yun J, Goh Y, Chung J. DQN-based optimization framework for secure sharded blockchain systems. IEEE Internet Things J 2020; 8:708–22.
83. Arulkumaran K, Deisenroth MP, Brundage M, Bharath AA. Deep reinforcement learning: A brief survey. IEEE Signal Process Mag 2017; 34:26–38.
84. Wu Y, Zhang N, Yan Z, Atiquzzaman M, Xiang Y. Guest editorial special issue on AI and blockchain-powered IoT sustainable computing. IEEE Internet Things 2023;10(8):6531–4.
85. Liu Y, Liu J, Li D, Yu H, Wu Q. Fleetchain: A secure scalable and responsive blockchain achieving optimal sharding. In: International conference on algorithms and architectures for parallel processing. 2020, p. 409–25.
86. Samaras G, Britton K, Citron A, Mohan C. Two-phase commit optimizations in a commercial distributed environment. Distrib Parallel Databases 1995; 3:325–60.
87. Li S, Yu M, Yang C, Avestimehr AS, Kannan S, Viswanath P. Polyshard: Coded sharding achieves linearly scaling efficiency and security simultaneously. IEEE Trans Inf Forens Secur 2020;16: 249–61.
88. Kopparty S, Ron-Zewi N, Saraf S, Wootters M. Improved decoding of folded reed-Solomon and multiplicity codes. In: 2018 IEEE 59th annual symposium on foundations of computer science. 2018, p. 212–23.
89. Liu G, Yan Z, Wang D, Wang H, Li T. DePTVM: Decentralized pseudonym and trust value management for integrated networks. IEEE Trans Depend Secure Comput 2023.
90. Liu K, Yan Z, Liang X, Kantola R, Hu C. A survey on blockchain-enabled federated learning and its prospects with digital twin. Digit Commun Netw 2022.
91. Feng W, Li Y, Yang X, Yan Z, Chen L. Blockchain-based data transmission control for tactical data link. Digit Commun Netw 2021;7(3):285–94. [122] Choo KKR, Yan Z, Meng W. Blockchain in industrial IoT applications security and privacy advances, challenges and opportunities. IEEE Trans Ind Inf 2020;16(6):4119–21.
92. Feng W, Li Y, Yang X, Yan Z, Chen L. Blockchain-based data transmission control for tactical data link. Digit Commun Netw 2021;7(3):285–94. [122] Choo KKR, Yan Z, Meng W. Blockchain in industrial IoT applications security and privacy advances, challenges and opportunities. IEEE Trans Ind Inf 2020;16(6):4119–21.

.