2

Related Work

Consensus algorithms are the core concept of blockchain technology. They facilitate the process of reaching an agreement on specific decisions or actions among the nodes in a blockchain network. This process ensures that the majority of nodes in the network validate and commit to the authenticity of transactions, making consensus algorithms vital for preserving the security and integrity of the blockchain ledger [53]. Various consensus algorithms, such as PoW, PoS, PBFT, and DPoS, are employed by different blockchain platforms. Broadly, these algorithms are categorized into two groups: Proof or resource-based consensus algorithms and Vote or authority-based consensus algorithms [13]. The state-of-the-art schemes either introduce novel consensus algorithms or present modified versions of existing ones. However, the primary objectives of these schemes are to enhance scalability, improve interoperability, or demonstrate the practical applications of blockchain in various domains such as IoT, ITS, and Smart Grids. Consequently, we categorize the related work into four areas: consensus enhancements, scalable blockchain schemes, interoperable blockchain schemes, and blockchain applications. The subsequent sections provide an in-depth exploration of these state-of-the-art schemes.

2.1 CONSENSUS ALGORITHM ENHANCEMENTS

There are many researchers who proposed a significant enhancement in the existing consensus algorithms, specifically the PoW, PoS, and the PBFT. Below are state-of-the-art schemes of blockchain enhancements. Peercoin [14] and BlackCoin [54] are the techniques that use the PoS for the consensus amongst the nodes. However, Peercoin is a peer-to-peer cryptocurrency utilizing both PoW and PoS systems. Some PoS cryptocurrencies require a digital signature to sign the block to mitigate the fork digitally. Fitzi et al. [55] proposed a formal execution model for PoS, which enables the expression of the near-optimal transactional throughput. The proposed modified version of the PoS protocol achieves security and optimal throughput against an active adversary who controls the stakes in the system. Kiayias et al. [56] improves the fundamental security threshold of PoS by following the longest chain rule and in the presence of honest and adversarial leaders. Bagaria et al. [57] proposed PoS longest chain protocols to ensure security against nothing-at-stake attacks and use the s-truncated longest chain rule to prevent attacks. However, there is a probability that adversaries could win all leader elections. Karakostas et al. [58] proposed a scheme to secure PoW against majority attacks using checkpointing to reduce the energy and computational resources required for mining. It leads to governance issues due to external entities for checkpointing. Kohlweiss et al. [59] proposed a anonymous PoS. It leverages network delays to distinguish stakeholders. It also

provides liveness guarantees under adversary-controlled network delays, enabling an adversary to determine a node's stake through message delays. However, it is not scalable in a permissionless blockchain setting because of the challenge of finding honest parties distributed across the network. The linear nature of blockchain ensures data security but restricts transaction processing speed. Therefore, Song et al. [60] presents a Layer-based directed acyclic (L-DAG) graph blockchain that maintains block order and employs a modified PBFT protocol. Using the proportional integral derivative controller, the L-DAG ensures ledger consistency. Implemented through Hyperledger Fabric, the L-DAG-based PBFT demonstrates near-linear efficiency in transaction processing as consensus threads increase. L. Daniel proposed a DPoS [11] scheme that relies upon a group of delegates to validate blocks on behalf of all nodes in the network. Coin holders use their coin balances to elect delegates, called witnesses. These witnesses (delegates) create blocks of new transactions and add them to the blockchain. However, it is not good for large networks because there are generally between 21–100 elected delegates in a DPoS system. A leaderless consensus [61] is proposed to avoid leader bottleneck and reduce the impact of a single point of failure on performance. Liu et al. [62] proposed an improved PBFT consensus called Credit (CBFT) enhanced with a grouping and credit model. It shows the low throughput as it is just 3.1 times that of PBFT, and latency is 7.4% that of PBFT. Xu et al. [63] describes a system that tolerates up to half of the nodes being adversaries, improving throughput with parallel shards. Many researchers used two different consensus algorithms for their solutions. Kogias et al. [64] proposed a PoW and PBFT-based consensus protocol called ByzCoin. It is an extension of Bitcoin-NG. A group of leaders generates key blocks instead of one leader. The achieved throughput is about 600-700 TPS with 1008 nodes, which is very low. Additionally, poor scalability and fork generation are the big concerns. A trusted finance supply chain data is proposed in [65]. It is suitable for public environments and mitigates financial risks by ensuring transparent and secure financial transactions.

2.2 STATE-OF-THE-ART SCHEMES FOR SCALABLE BLOCKCHAIN

Bitcoin is the first broadly adopted cryptocurrency that uses the PoW [1] consensus algorithm to agree on the validation of the transactions. In Bitcoin, PoW takes 10 minutes to add every next block into the blockchain ledger [66], [67], and it takes approximately one hour or at least six blocks to confirm the transaction [68], [69]. Hence, the throughput is very low. Bitcoin-NG [70] solves this issue of Bitcoin and proposes a new protocol that uses the PoW for leader selection. It uses two types of blocks, key block and microblock, and the operation is organized into periods called epochs. The distinction between a microblock and a key block is that the key block does not contain any transaction, but the microblock does. The key issues of Bitcoin-NG are the unfair selection of leaders, the remuneration policy, and the higher possibility of forks. The ByzCoin [64], which is based on the PBFT protocol, extends the Bitcoin-NG [70] to achieve high transaction throughput. The key block generation has been modified, where the group of leaders generates the key block instead of a single leader. The remuneration model also changed where the incentives are distributed within the peer nodes in proportion to their stakes. The leader runs a modified version of the PBFT to generate a combined signature that confirms at least two-thirds of valid responses. A node can verify in constant time that the consensus group has validated a macroblock. A milestone approach called Algorand [71] is a byzantine agreement protocol that uses Verifiable Random Functions (VRF) for the selection of nodes for consensus. Algorand's achieved throughput is 125 times that of Bitcoin. Obscuro [72] provides anonymity to Bitcoin transactions. The trusted execution environment gives high efficiency to the protocol. Conflux [73] enhanced the performance with high throughput and fast confirmation time using a scalable solution. Conflux arranged the blocks in a Tree-Graph structure. In Tree-Graph, the blocks

Table 2.1: Comparison of consensus algorithm enhancements

Scheme	Consensus Algorithm	Advantages	Limitations
Peercoin [14]	PoS	First peer-to-peer cryptocurrency based on PoS reduces the energy consumption of PoW by limiting the hashing search space	1. Potential misuse of the coin age concept. 2. Potential centralization due to centralized checkpointing
BlackCoin [54]	PoS	It is PoS version-2 that resolves the issues of original PoS, which is adversarial use of coin age	Potential susceptibility to attacks due to lower proof computation
Fitzi et al. [55]	PoS	Near-optimal transactional throughput against active adversaries	Adversarial stake control pose risks
Kiayias et al. [56]	PoS	Improved security threshold by honest/adversarial leader distinction	Adversarial control during leader elections
Karakostas et al. [58]	PoW + Checkpointing	Reduces energy/resource usage, enhances security	Governance issues due to external entities, potential centralization
Kohlweiss et al. [59]	PoS + Anonymity	Used the PoS with anonymity and ensures liveness under network delays and privacy preservation	Not scalable in permissionless settings and network delay reveals stakes
Song et al. [60]	PBFT + L-DAG	Used the PBFT consensus along with layered based DAG structure and provides near-linear transaction processing	Complex implementation, limited to Hyperledger environments
L. Daniel [11]	DPoS	Relies upon a group of delegates to validate blocks on behalf of all nodes in the network. Coin holders use their coin balances to elect delegates, called witnesses. These witnesses (delegates) create blocks of new transactions and add them to the blockchain.	Not good for large networks because there are generally between 21–100 elected delegates in a DPoS system. Fast compared to PoS but partially centralized.
Antoniadis et al. [61]	Leaderless Consensus	Used leaderless consensus to avoid leader bottleneck and enhances fault tolerance	Potentially higher communication overhead, complexity in implementation
Liu et al. [62]	PBFT + Credit (CBFT)	This also used PoW and PBFT together for transparent and secure financial transactions	Architectural design leads to potential centralization and high consensus delay
Xu et al. [63]	PoW + Parallel Sharding	Tolerates up to half nodes as adversaries, improved throughput	Complexity in sharding management, cross-shard communication issues
Kogias et al. [64]	PoW + PBFT (ByzCoin)	Used the PoW and PBFT in conjunction to improve throughput and distributed incentive model	Issue of forking and potential double-spending
Liu et al. [65]	PoW + PBFT	Transparent and secure financial transactions	High consensus delay, potential centralization

are linked based on the happened-before relationship; thus, concurrent blocks are not considered conflicts. The block confirmation time is about one minute, which can significantly reduce to achieve high throughput. Another protocol called OmniLedger [74], a sharding-based distributed ledger scheme, was proposed, which introduces a cross-shard commit protocol for intra-shard transaction processing.

Monoxide [75] runs multiple independent and parallel instances of single-chain consensus systems termed zones. However, these zones are susceptible to double spending and forking attacks. HoneyBadger [76] proposed by Miller et al. assigns a collection of servers to reach consensus for validated transactions. The achieved throughput is 1500 transactions per second with 104 nodes. The scheme also shows the high consensus delay and partial centralization. A scheme called RedBelly [77] proposed by Crain et al. claims to be fork-proof. A lack of decentralization and trust is identified due to the restricted participation of pre-approved nodes. RapidChain emphasizes fully sharded solutions [78], while ELASTICO offers a secure sharding protocol for open blockchains [79]. Chainspace focuses on transaction processing with a unique node structure [80], and research stresses the importance of shard-persistence and shard-liveness for maintaining safety and liveness in transactions [23]. PBFT's frequent inter-node communications hinder its scalability, making it suitable for smaller networks. To address this, Li et al. [81] introduce a scalable multi-layer PBFT mechanism that hierarchically groups nodes into different layers, restricting communication within these groups. An optimal double-layer PBFT is proposed, which minimizes communication complexity when nodes are evenly distributed within the second layer's sub-groups. Marson et al. [82] proposed a novel schemes for scaling blockchain called Mitosis that enhances throughput by dynamically splitting and merging blockchain shards based on network demand. Mitosis achieves high scalability and maintains security through a combination of parallel processing and a consensus protocol designed for sharded blockchains, making it a robust solution for large-scale distributed networks. The major drawback of Mitosis is the complexity of managing shard splits and merges, which can lead to increased latency and potential inconsistencies during high-traffic periods. Gazi et al. [83] proposed a blockchain transaction settlements estimation that facilitates trust in decentralized systems, which supports scalability. However, it is resource-intensive. Cai et al. [84] proposed a scheme called Benzene for scaling blockchain With a cooperation-based sharding design for a cross-shard block verification mechanism leveraging a Trusted Execution Environment (TEE). Yu et al. [85] proposed a sharding approach called Overshard for scaling blockchain that incorporates an overlapping network. The overlapping network model enables all nodes in a shard to join multiple other shards. Due to the incorporation of overlapping networks, the communication overhead is higher. Singh et al. [86] proposed a blockchain-based decentralized trust management scheme using smart contracts. Specifically, the author introduces the concept of blockchain sharding to reduce the load on the main blockchain and increase the transaction throughput. However, the high sharding overhead poses a significant hurdle in achieving high performance. Bagaria et al. [87] proposed a novel blockchain protocol called PRISM that decouples traditional blockchain architecture into proposer, transaction, and vote blocks. This multi-block approach enables high transaction throughput and fault tolerance, significantly improving scalability and efficiency. However, the added complexity and resource intensity pose challenges in implementation and maintenance. The PRISM authors further improve the PRISM protocol's blockchain performance in [88] and [89]. They aim to scale Bitcoin by a factor of 10,000. The protocol introduces optimizations for proposer block generation, parallel processing of transaction blocks, and an enhanced vote block mechanism, achieving unprecedented scalability and robustness. Nevertheless, this scalability comes at the cost of increased network overhead and potential synchronization issues. A common bottleneck of the above schemes is that they face a high cross-shard communication overhead in sharding blockchain. Additionally, the biased leader selection is prone to many vulnerabilities. Consequently, these state-of-the-art schemes face the performance issue, i.e., low throughput. Some of the schemes improved the performance of blockchain using the sharding concept. However, incorporating sharding brings new

challenges to the blockchain, such as cross-shard communication overhead and shard takeover attacks. As a result, the performance has not improved as expected. The proposed solutions BlockTree and UnoShard address these challenges in the sharding-based blockchain.

2.3 STATE-OF-THE-ART SCHEMES FOR INTEROPERABLE BLOCKCHAIN

Blockchain technology's rapid evolution has extended its impact beyond cryptocurrencies, creating a growing need for interoperability among the increasing number of blockchain platforms. Interoperability is crucial for enabling seamless asset transfers, data sharing, and communication across different blockchain ecosystems. The survey papers [27], [28] provide a comprehensive overview of the current state of blockchain interoperability, which states that interoperability approaches can be categorized into various types, including sidechains, notary schemes, hash-locking, and blockchain of blockchains. They also highlight key challenges, such as standardization, security, and the presence of a third party as an intermediary, which must be addressed to achieve effective interoperability. Developing universal standards and more robust protocols is essential for overcoming these limitations and advancing blockchain interoperability. In this section, we have provided detailed and comprehensive work related to state-of-the-art schemes that addressed various issues of blockchain interoperability. Zamyatin et al. [90] provides a systematic overview of communication protocols between distributed ledgers focusing on achieving secure and efficient interoperability. The study concludes that while significant progress has been made, there is still a need for more robust and scalable communication protocols to support widespread blockchain interoperability. A novel platform for smart contracts and decentralized apps for enabling interoperability across multiple blockchains has been done by the makers of Ethereum in [6]. Kwon et al. [91] designed a system called Cosmos that aims to address the challenges of blockchain scalability and interoperability by enabling cross-chain communication while retaining the security properties. However, its reliance on the Cosmos Hub as a central point of failure could pose risks. Gazi et al. [83] addressed the challenge of determining settlement times in blockchain systems, which is critical for ensuring secure and reliable cross-chain transactions. However, this approach is limited by the inherent delay and energy inefficiencies associated with PoW mechanisms, which hinders its applicability in high-throughput interoperability scenarios. Jin et al. [92] proposed an architectural framework designed to facilitate interoperability and emphasize modularity, allowing different blockchain systems to integrate through standardized interfaces. While the architecture offers a flexible solution to interoperability, it is still in the conceptual stage and lacks a practical implementation that can demonstrate its effectiveness in real-world scenarios. Pillai et al. [93] introduced a protocol called Burn-to-Claim, a novel approach to asset transfer across multiple blockchains by requiring assets to be burned on the source blockchain before being claimed on the destination blockchain. Burn-to-Claim addressed the double spending challenges by ensuring that assets are not duplicated across chains. However, the protocol's reliance on asset burning can be seen as a limitation, as it permanently removes assets from the source blockchain, which may not be suitable for all use cases. Su et al. [94] accomplish the task of cross-chain exchange using transaction dependencies and conditional transactions. The approach allows for the secure exchange of assets across blockchains without the need for a trusted third party. However, this scheme is very complex to implement and requires all participating blockchains to support conditional transactions, which limits its applicability. Sigwart et al. [95] used the combination of atomic swaps and smart contracts to design a fully decentralized protocol for asset transfer between blockchains without the need for intermediaries. Although this approach enhances security and decentralization, it suffers from scalability issues, particularly when dealing with a large number of transactions or blockchains. Besanccon et al. [96] proposed a framework

Table 2.2: Comparison of state-of-the-art schemes for scalable blockchain

Scheme	Consensus Algorithm	Description	Limitations
Bitcoin-NG [70]	PoW	Decouples blockchain operation into Leader selection and transaction serialization Two types of blocks, keyblock and microblock	Unfair leader selection and remuneration policy, potential fork generation, and low throughput up to 20 TPS.
ByzCoin [64]	PoW + PBFT	An extension of Bitcoin-NG Group of leader generate key block instead of one leader. Remuneration is distributed based on stakes	Poor Scalability, fork generation, low throughput 600-700 TPS with 1008 nodes
Algorand [71]	VRF + Byzantine Agreement	Byzantine agreement protocol called BA*. Uses Verifiable Random functions for the selection of nodes for consensus	Dependency on VRF security and low throughput as of 125 times Bitcoin's throughput
Conflux [73]	PoW + Tree-Graph	Conflux operates with a novel consensus protocol which optimistically processes concurrent blocks without discarding any as forks and adaptively assigns weights to blocks based on their topologies in the Conflux ledger structure (called Tree-Graph)	Complex structure and vulnerability to double-spending attacks
OmniLedger [74]	ByzCoinX	Sharding based distributed ledger scheme. Introduce cross-shard commit protocol Parallel intra-shard transaction processing	Potential shard takeover attacks, fork generation, low scalability
Monoxide [75]	Asynchronous Consensus Zones	Running multiple independent and parallel instances of single chain consensus systems termed as zones	Double spending attack due to independent consensus zones and low scalability
HoneyBadger [76]	Asynchronous BFT	Assigns a collection of servers to reach consensus for validated transactions	Partial centralization, High consensus delay, 1500 TPS with 104 nodes
RedBelly [77]	PBFT	Fork-proof, high security	Centralization risks, restricted participation
RapidChain [78]	Optimal intra-committee consensus	Fully sharded solution, high scalability	Cross-shard communication overhead, shard takeover risks
ELASTICO [79]	Classical byzantine consensus	Secure sharding, suitable for open blockchains	High overhead in shard communication, potential for attacks
Chainspace [80]	Sharded Byzantine Atomic Commit (S-BAC)	Node structure optimized for transaction processing	Complexity in shard-persistence and shard-liveness management
PRISM [87]	Proposer-Transaction-Vote Blocks	Prism is based on a structured DAG created by cryptographic sortition of the mined blocks. Divided the process into three steps: proposer block, voter block, and transaction block	Increased network overhead and potential synchronization issues. Added complexity and resource intensity pose challenges in the implementation

for secure data exchange across gaming platforms, allowing players to transfer assets between different gaming environments. However, its focus on a niche area limits its broader applicability. In [97], a pegged sidechains concept was proposed as a more general solution for blockchain interoperability, enabling asset transfers between blockchains without altering the underlying protocols. While promising, this approach presents challenges in maintaining the security and stability of the sidechains. Zarick et al. [98] proposed a novel protocol called LayerZero, which is a trustless omnichannel interoperability protocol. This protocol achieves direct cross-chain transactions without replying to a trusted third party. However, while the approach is innovative, it introduces potential challenges related to the reliance on off-chain entities, which, though independent, could become points of failure or attack in certain scenarios. Xie et al. [99] proposed a novel approach called zkBridge using zk-SNARK. The zkBridge is scalable and privacy-preserving, making it suitable for use in scenarios where data confidentiality is crucial. However, the scheme is computationally inefficient as it shows a high computational overhead. Liu et al. [100] proposed an interoperability platform called HyperService specifically designed for Daaps. The platform used a two-layer architecture consisting of a control layer that manages cross-chain transactions and a data layer that handles the execution of smart contracts. The scheme is highly susceptible to a single point of failure due to the centralized control layer. Despite significant advancements proposed by state-of-the-art schemes for blockchain interoperability, they often fall short in many key areas, such as these solutions being either confined to specific ecosystems or suffering from performance bottlenecks, which limits their applicability in diverse blockchain environments. In contrast, the proposed *CrossLedger* is a comprehensive interoperability solution that overcomes the limitations of these state-of-the-art schemes. *CrossLedger* integrates advanced security features such as atomicity, non-repudiation, unlinkability, and confidentiality, ensuring secure and private cross-chain transactions. Unlike other solutions, it offers true interoperability across various blockchain platforms without requiring significant modifications to existing protocols, providing greater flexibility.

2.4 STATE-OF-THE-ART SCHEMES FOR BLOCKCHAIN APPLICATION

Blockchain technology can be adopted in various applications, including IoT, ITS, and smart grids. Numerous schemes have been proposed in these areas to enhance the performance and security of these applications. In this related work section, we explore several such schemes, discussing their merits and demerits. Hammi et al. [101] proposed a decentralized authentication mechanism called Bubble of Trust, creating secure virtual zones for the IoT application. The high computation overhead, storage overhead, and low throughput are the big concerns of this scheme. Dorri et al. [102] proposed a lightweight and scalable blockchain that forms an overlay network of IoT devices. Another application for IoT is proposed called IoT passport [103], which is a decentralized trust framework for cross-platform collaboration motivated with real, real-life passport system rules written in smart contracts. The low scalability and high computational overhead are the issues of this scheme. Li et al. [104] proposed a blockchain-based data storage and protection scheme. It used the distributed hash table to store the data and blockchain to handle the device's authentication. The computation and storage overhead is very high for lightweight IoT devices. Mirsky et al. [105] proposed anomaly detection using blockchain to ensemble an anomaly detection model for distributed trust. The extensible markov model is used for anomaly detection training. High computation overhead, high consensus delay, and poor scalability are the main concerns of this scheme. Yang et al. [106] proposed a decentralized trust management system in vehicular networks based on blockchain techniques, i.e., PoW and PoS. The Bayesian inference model is used to validate the messages received by the neighboring vehicles. Lau et al. [107] proposed the blockchain-based authentication scheme in the IoT

Table 2.3: Comparison of state-of-the-art schemes for interoperable blockchain

Scheme	Consensus Algorithm	Description	Limitations
Zamyatin et al. [90]	Various (Communication protocols)	Cross-chain communication focusing on achieving secure and efficient interoperability	Limited robustness and scalability
Cosmos [91]	Tendermint	Addressed the challenge of scalability and interoperability by enabling cross-chain communication while retaining security	Potential risk of a single point of failure due to reliance on central Cosmos Hub
Burn-to-Claim [93]	Asset burning mechanism	Introduced protocol called Burn-to-claim, to asset transfer across multiple blockchains and prevents double spending, ensure asset uniqueness	Permanent asset removal from source blockchain results to limited use cases
LayerZero [98]	Trustless omnichannel protocol	Proposed a protocol called LayerZero, a trustless omnichannel interoperability protocol, enables direct transfer with trusted third party	Potential challenge on reliance on off-chain entities, which could become the point of failure and attract attackers
zkBridge [99]	zk-SNARK	Proposed a protocol zkBridge using cryptographic tool zk-SNARK, is a scalable and privacy-preserving suitable for scenarios where data confidentiality is crucial	Computationally inefficient due to high computational overhead.
HyperService [100]	Two-layer architecture	Proposed interoperability platform called HyperService specially designed for Dapps, which used the two-layer architecture	Single point of failure due to centralized control layer

network to authenticate IoT devices when they join the IoT network. The authenticated device configuration protocol (ADCP) is proposed for authentication. However, there is no mechanism to check the integrity of the information, and the scheme is prone to Sybil attacks. Michelin et al. [108] proposed a scheme called SpeedyChain for smart cities to secure the data. They have used the permissioned blockchain. The proposed scheme mainly focused on ITS's security, which is unsuitable for a heterogeneous environment. Cui et al. [43] proposed a hybrid blockchain-based identity authentication scheme for IoT networks. Different types of nodes in the network form the hybrid blockchain network, say local blockchain and public blockchain. However, the scheme is not fully decentralized and, hence, prone to single-point failure. The message size is also very high, approximately 30-350MB, which is huge for the IoT network. Gao et al. [109] proposed a scheme for vehicular networks using blockchain and software-defined networks to enhance network performance and establish trust among peer nodes. Zhang et al. [110] proposed a secure data sharing scheme for the IoV network. The scheme encourages honest participants to give incentives in the form of some cryptocurrency. However, the scheme used the central trusted management authority, which again violates the concept of blockchain, i.e., distributed system, and is highly prone to single-point failure. Additionally, the system's throughput depends on the underlying cryptocurrency, which will be very low if Bitcoin and Ethereum are used. The proposed algorithm used PoW for the leader selection and the PBFT for the consensus on the transactions' finality. Li et al. [111] proposed an incentive announcement scheme for vehicular networks based on blockchain technology called CreditCoin. There is a central, trusted authority that can

be compromised. Trust-based blockchain technology, along with deep learning techniques [112], has been used by researchers to improve the consensus mechanism in software-defined vehicular networks. Huang X. et al. [113] proposed a blockchain-based security model for electric vehicle and charging pile management, i.e., the security of trading between the electric vehicle and charging pile. Kudva S. et al. [114] proposed a secure and practical consensus algorithm called proof of driving (PoD) to address the efficiency, fairness, and scalability issues of PoW, PoS, and PBFT consensus algorithms for blockchain-based VANET systems. The PoD was designed to randomize the selection of honest miners for block generation. The author also introduced a filtering technique based on the service standard score of the vehicular miner nodes to detect and eliminate malicious nodes. An Efficient privacy-preserving authentication model has been proposed in [115] to tackle the problem of high latency membership verification for users in VANET for confidential identity requirements. It is a three-phase process where the first phase is initialization, the second phase is chain construction, and the third phase is authentication. Similarly, in [116], a privacy-preserving vehicular communication is proposed in a combination of consortium blockchain and edge computing to support efficient computation and storage capabilities with low communication delay. To achieve privacy preservation, a pseudonym mechanism is utilized, and an identity-based signature is used to achieve the authentication of vehicles. In [117] author proposed reputation management for a cloud-based IoV system. Routing based metrics are being used to monitor the vehicles and, based on that, update their reputations. Based on the reputation, a certificate is issued to show trust in the vehicular system.

Many researchers have integrated blockchain to address the centralization issue in smart grids. Liang et al. [118] enhanced the smart grid's defence against cyberattacks using a blockchain-based security framework. However, it's not fit for lightweight devices like smart meters due to its high processing time, computational cost, and consensus delay. Jindal et al. [119] introduced a blockchain-based smart grid scheme called "guardian," but its PoW consensus algorithm has a prolonged confirmation time, making it unsuitable for smart grid use. Wang et al. [120] presented anonymous authentication with key management, but its cryptographic approach is computationally intensive for devices like smart meters. While these methods address the smart grid's centralization, their consensus delays are too long, and throughput is too low for optimal smart grid operations. Wang et al. [121] suggested using smart contracts and delegated consensus mechanisms for smart grid trading, emphasizing fairness and a reputation system for P2P trading. However, its consensus algorithm, similar to PoW, is computationally intensive. Guan et al. [122] introduced a privacy-preserving energy trading scheme using blockchain and attribute-based encryption. They also presented a credibility-based equity-proof consensus algorithm to boost efficiency.

Yang et al. [123] introduced a consortium blockchain trading mechanism for P2P energy trading based on a PoS protocol. They employed smart contracts and launched a cryptocurrency named "elecoin" for the P2P market. Similarly, Cao et al. [124] presented a solution addressing credit and security concerns in energy trading, utilizing elecoins to optimize the utility of energy traders. Their approach models the elecoins-purchasing dilemma as a hierarchical Stackelberg game. A miner reward mechanism was suggested in [125] for energy trading. This paper recommends a consortium blockchain system using a PoS consensus algorithm to ensure secure, transparent energy transactions and reduce trading costs. They also introduced the elecoin cryptocurrency for P2P trading within microgrids. These state-of-the-art schemes are prone to various attacks in the blockchain application environment. Karumba et al. [126] introduced HARB, a hypergraph-based framework for energy trading using consortium blockchain. HARB's three-layered network architecture addresses scalability and distributed trust issues in energy trading communities. AlSkaif et al. [127] introduced a peer-to-peer energy trading strategy for residential systems, determining bilateral trading preferences based on surplus power matching and trader distance. Ping et al. [128] presented a privacy-preserved Optimize Energy Trading (OET) scheme using blockchain. They proposed a privacy-

preserving byzantine fault tolerance coordination algorithm to account for dishonesty and ensure accurate trading results. Christidis et al. [129] introduced a framework for creating a blockchain-based local energy market, highlighting that the blockchain type significantly impacts energy distribution and trading performance. However, this framework faces scalability issues. Guo et al. [130] proposed an architecture for distributed energy trading on a byzantine-based blockchain, leveraging the PBFT consensus algorithm and smart contracts. However, the PBFT-based model is deemed inefficient due to high message overhead. Many state-of-the-art schemes used auction mechanisms to further enhance energy trading in the smart grid.

Nguyen T. et al. [131] discusses an Ethereum blockchain-based framework for iterative double auction that's trustless and decentralized. It boasts low latency and fee-less on-chain transactions. Chen Z. et al. [132] introduce a fair cloud auction design using blockchain, achieving financial fairness through a timed commitment scheme with deposits. However, this design exposes other parties' bids, leading to potential bid-rigging. Generally, blockchain and double auction systems risk exposing sensitive buyer and seller information. In contrast, our auction approach in the proposed scheme ETradeChain is budget-balanced, fair to all participants, lightweight, and decentralized in bid allocation, relying on the entire peer network. Singla S. et al. [133] also used the Virkrey-Clarke-Groves Auction for efficient energy trading along with providing the fair optimal pricing algorithm that does not discriminate and increases social welfare. However, it also has a centralized auctioneer, which can have a single point of failure problem. Ma et al. [134] used a blockchain-based distributed Feedback-based Combinatorial Multiunit Double Auction (FC-MDA) mechanism for trading the resources of the cloud. The state-of-the-art schemes faced performance bottlenecks due to design issues in the PBFT and other modified versions of PBFT. The issues are unbiased leader selection, improper reward distribution, and high message overhead complexity. Therefore, to solve the issues, we have proposed various schemes. For IoT applications, we have proposed BLISS, BSS, and SCAB-IOTA, which solve the issues of authentication and secure communication of devices. For ITS, we have proposed LBSV and SmartCoin, which provide secure communication and enable efficient micropayments within intelligent transportation networks. For the Smart Grid, SmartGrid-NG, ETradeChain, and $zk-SGB$ were proposed to facilitate secure energy trading and efficient grid management. Each technique was designed to address specific challenges within its respective domain, demonstrating the versatility and potential of blockchain in improving various aspects of smart city infrastructure.

Concluding Remark

In this chapter, we comprehensively reviewed the existing literature on blockchain scalability, interoperability, and applications, identifying the limitations and gaps in current research. We explored various consensus algorithms, such as PoW, PoS, PBFT, and DPoS, and discussed their strengths and weaknesses. Additionally, we examined the current state of blockchain applications in domains like IoT, ITS, and smart grids. The findings highlighted the need for innovative solutions to address the scalability and interoperability challenges that hinder the widespread adoption of blockchain technology. These insights form the foundation for the subsequent chapters, where we propose novel techniques to overcome these challenges. In the next chapter, we focus on enhancing the scalability of blockchain networks through the development of BlockTree and UnoShard, which aim to improve transaction throughput and overall efficiency.