frontiers | Frontiers in Blockchain

TYPE Review
PUBLISHED 27 February 2023
DOI 10.3389/fbloc.2023.996070

OPEN ACCESS

EDITED BY
Qingyi Zhu,
Chongqing University of Posts and Telecommunications, China

REVIEWED BY
Rameez Asif,
University of East Anglia, United Kingdom
Bhagwan Chowdhry,
Indian School of Business, India

*CORRESPONDENCE
Feng Liu,
lsttoy@163.com

SPECIALTY SECTION
This article was submitted to Blockchain Technologies, a section of the journal Frontiers in Blockchain

RECEIVED 17 July 2022
ACCEPTED 09 February 2023
PUBLISHED 27 February 2023

CITATION
Liu F, He S, Li Z and Li Z (2023), An overview of blockchain efficient interaction technologies.
Front. Blockchain 6:996070.
doi: 10.3389/fbloc.2023.996070

An overview of blockchain efficient interaction technologies

Feng Liu[1,2]*, Sihao He[3], Zhenghao Li[3] and Zhibin Li[1,2]

[1]Shanghai International School of Chief Technology Officer, East China Normal University, Shanghai, China, [2]School of Computer Science and Technology, East China Normal University, Shanghai, China, [3]Institute of Artificial Intelligence and Change Management, Shanghai University of International Business and Economics, Shanghai, China

The successful operation of Bitcoin has made its underlying blockchain technology receive wide attention. As the application scenarios of blockchain technology are enriched, the requirements for its performance are getting higher. Therefore, it is of utmost importance to effectively solve the problem of high-performance data interaction in the blockchain. In this paper, based on relevant domestic and foreign research literature, we start from the development history of blockchain technology and review the relevant research work on improving the performance of blockchain from three perspectives: on-chain interaction technology, off-chain interaction technology, and cross-chain interaction technology in turn. The on-chain and off-chain interaction technologies improve performance by improving the architecture of the blockchain system. The performance improvement solution of on-chain interaction technology is to modify and optimize the basic protocol and architecture of the blockchain itself to achieve a performance improvement. Still, the impact of this approach is limited in terms of performance improvement. The performance improvement solution of off-chain interaction technology is to transfer part of the data processing to off-chain and only return the final result to on-chain for storage and recording, which reduces the burden of on-chain operation and improves the efficiency of data processing. In terms of cross-chain interaction technology, this paper analyses four mainstream technology, namely, Notary Scheme, Side chain and Chain relay, Hash-Locking, and Distributed Private Key Control, and ultimately concludes through comparative analysis that cross-chain technology has a significant impact on improving blockchain performance. Finally, the paper provides a systematic overview of the above and an outlook on the possible future development of technologies related to enhancing blockchain performance.

KEYWORDS

blockchain, efficient interaction, on-chain technology, off-chain technology, cross-chain technology

1 Introduction

A user named "Satoshi Nakamoto" started the blockchain technology (BT) by proposing a decentralized Bitcoin system in a paper published on the internet called "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008). In simple terms, blockchain is a chain data system that connects blocks containing data in chronological order. It ensures the anonymity of data by using cryptography (2) principle, and makes the system decentralized by managing the authority of nodes in the whole network through consensus protocol. Based on BT, various approaches have been established to apply to finance, supply chain, government and other areas. Although BT has many excellent features and can solve

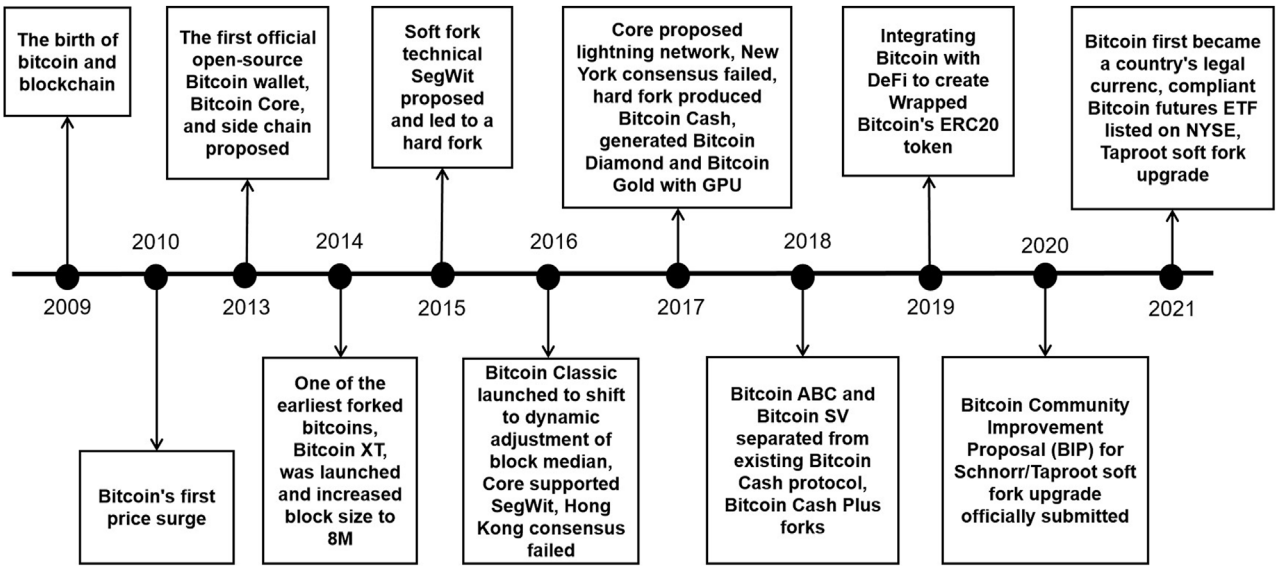

FIGURE 1
The development process of Bitcoin technology.

many practical problems, if we really want to make its robust large-scale application, we must consider its interaction efficiency and application deployment. In different development stages of BT, its interaction efficiency has always been the focus of academia and industry. Currently, the existing blockchain generation technologies can be divided into three categories: Blockchain 1.0, Blockchain 2.0 and Blockchain 2. x. Among the Blockchain 2. x generation, in addition to the technological development of single-chain, there exist various technological solutions represented by cross-chain technology to try to solve the efficiency bottleneck problem of blockchain.

1.1 Intergenerational development of BT

Blockchain 1.0 (shown in Figure 1) is a cryptocurrency represented by Bitcoin, encrypted by the trader's private key for transactions, allowing any transaction to be completed directly by both parties through the blockchain without needing third-party management. For the Bitcoin network, the system's efficiency, security and fairness can be assessed by four performance metrics: transaction throughput (TPS), network latency, number of forks and mining rewards. Most existing studies assessing the performance of the Bitcoin network have focused on the impact of block dissemination latency concerning the number of forks generated and its concomitant impact on network security and availability (Decker and Wattenhofer, 2013; Neudecker and Hartenstein, 2019; Shahsavari et al., 2019; Sompolinsky and Zohar, 2015). With the technological development of blockchain 1.0, people started to develop emerging applications beyond cryptocurrencies on blockchain systemsHowever, stability, efficiency and performance have not been a concern by people (Lone and Naaz, 2020). The blockchain, which originated from the underlying technology of Bitcoin, has a single function because it focuses on transactions and has not yet paid attention to the performance of the block itself and traceability. With the emergence of blockchain 2.0 technology mainly based on Ethereum, especially with its Turing-complete smart contract technology, BT has broken the limitation of being unable to break through the closed loop of its information in the past.

Ethereum, a representative technology of Blockchain 2.0 (shown in Figure 2) with programmable smart contract technology, has its code transaction protocol that passively executes contract terms to complete transactions based on logical conditions (Wood, 2014) that opens up a new era of interaction with real-world technologies. Transactions are initiated based on blockchain by multi-party agreements with electronic signatures, and smart contracts embedded with contractual terms and conditions are invoked after broadcast at each node of the blockchain network to function by executing computer programs. With the help of Ethereum technology, BT has been applied to other fields. Gradually, private and consortium chains have emerged that meet the needs of each industry itself, such as business processes (Prybila et al., 2020), data source traceability (Ruan et al., 2019; Sigwart et al., 2019; LIU Jia-qi and LIU, 2022), supply chain management (Tian, 2016), healthcare (Mettler, 2016), and intellectual property (Ajay et al., 2018). However, the representative platforms of blockchain 2.0, such as Ethereum in the data layer and consensus layer, need to be optimized in terms of algorithm mechanism, accommodation capacity and execution mode, and the performance bottleneck needs to be addressed at the architectural level (Wang and Chu, 2020). Meanwhile, not only does the network architecture affect the efficiency and system performance of satisfying contract execution, but the execution space inside the system limits the connection between contracts and off-chain data, resulting in the inability to link data assets between multiple chains.

The consortium chain (shown in Figure 3) can act as a transition technology between blockchain 2.0 and blockchain 3.0 and is often

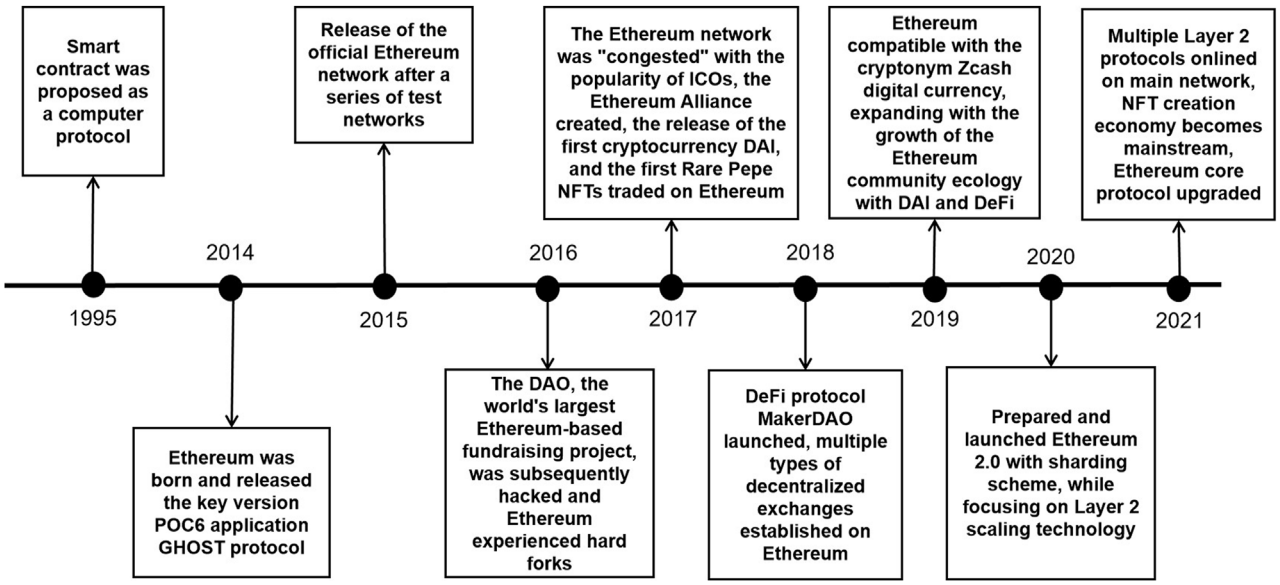

FIGURE 2
The development process of Ethereum technology.

considered blockchain generation 2. X (Buterin, 2015), thus laying the foundation for cross-chain and multi-chain technologies. The consortium chain can be used in industry-specific alliances or organizations that collaborate and maintain the blockchain and have higher requirements for security and performance. The Hyperledger Fabric system is a typical example of the consortium chain, which allows only licensed business alliances to organize, share and maintain the system, emphasizes collaboration between organizations in the same industry or across borders while not being fully decentralized, and is an important direction for the future development of blockchain. The consortium chain is oriented to specific industrial applications. It has the feasibility of commercial implementation as a form of combining BT with business in various fields, enabling the circulation of data such as transaction assets and providing credible services to various customers. However, there are still obvious performance bottlenecks in the existing consortium chain technology (Chen et al., 2020). At the same time, there are still significant limitations in data interaction with public chains (Buterin, 2016).In short, in the blockchain 1.0 era, people bought and sold cryptocurrencies for the difference in return and did not link cryptocurrencies to the value of applications and the digital ecology of the blockchain system. In the blockchain 2.0 era, technologies like Ethereum can build smart contracts to achieve programmable functions, focusing more on specific application logic and emphasizing performing tasks such as transactions through logical conditions. As decentralized blockchain technologies are applied in more complex domains, blockchain systems have emerged in addition to fully open public chains and consortium chain technologies in the blockchain 2. X generation that requires permission to use them. The consortium chain realizes the interconnection between multiple chains to a certain extent. Further, it enhances the operational efficiency of BT, which can serve as a transition technology between blockchain 2.0 and 3.0 and promote the construction of a perfect blockchain ecology. Although high-performance blockchain technologies have also continued to emerge in recent years, such as Polkadot technology, which is capable of handling slightly more than 1,000 transactions per second (Akintade, 2022), there is a significant performance gap with the throughput requirements of centralized banking systems such as MasterCard at 60,000 transactions per second (mastercard, 2020). Blockchain 3.0 intergenerational technology should open up the channel between multiple chains, which can significantly enhance the interactive performance based on ensuring the security and privacy of data interaction (Furfaro et al., 2019) that ultimately meets the real needs of BT landing on real-life scenarios. Therefore, in addition to the rapid development of single-chain technology, cross-chain technology has become a hot topic for researchers (F et al., 2019).

1.2 The development of blockchain cross-chain technology

Cross-chain technology is seen as one of the important means to achieve the need for interaction and improve the blockchain's overall efficiency. Currently, blockchains are gradually forming a chain network (Tam Vo et al., 2018) in the continuous development of blockchains, where people try to connect various blockchain systems to break the phenomenon of "value island" and give full play to the role of blockchain, and thus cross-chain technology has emerged.

As shown in Figure 4, in the early days of blockchain, industry-wide research on performance optimization and technology and storage upgrades for BT was based on single-chain research (Zhao et al., 2020), such as hard forking Bitcoin to improve consensus protocols. Later, as the demand for BT application scenarios

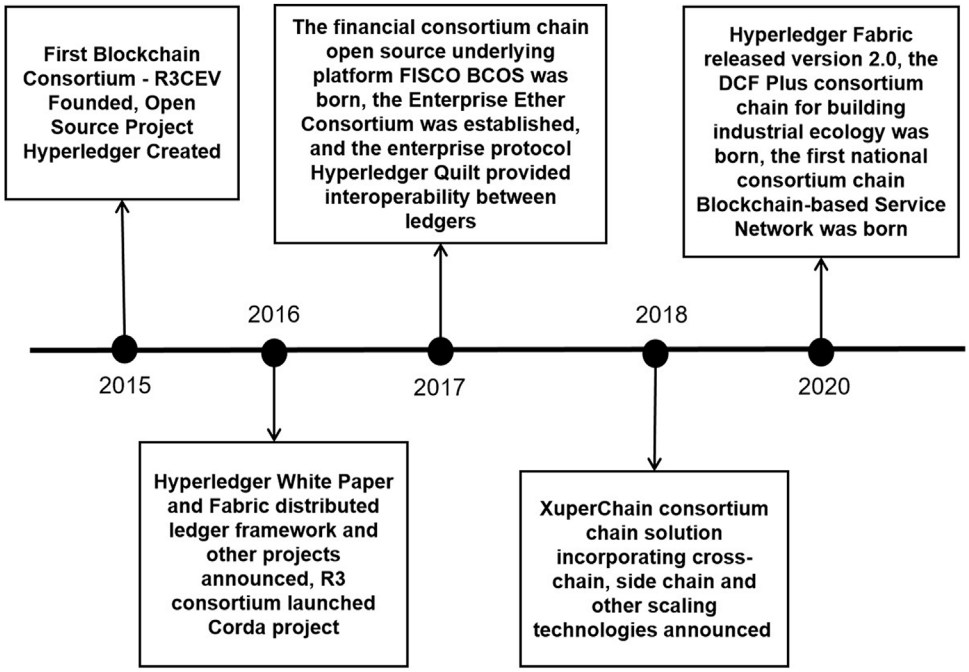

FIGURE 3
The development process of consortium chain technology.

increased, the industry began to research single-chain performance enhancement. Firstly, in 2012, Ripple proposed an early version of the Interledger Protocol (Schwartz et al., 2014; Thomas and Schwartz, 2015) to link different blockchain ledgers and thus exploit synergies. In the following years, related theories such as atomic transfer (Collado et al., 2013) and sidechaining emerged to further improve the performance of single chains. In particular, the hashed time lock (Kang et al., 2007), which emerged in the Bitcoin lightning network in 2015, enabled fast transaction channels under the Bitcoin chain and greatly improved the transaction efficiency of the Bitcoin system. Since 2016, many companies have launched cross-chain platforms to connect numerous blockchains through one system to form a chain network. In 2016, the BTC-Relay (Kwon and Buchman, 2016) program was released based on the Relay Cross-chain protocol and enabled a one-way cross-chain connection from Bitcoin to Ethereum. Cross-chain has remained a hot topic in BT in recent years. Both the Cosmos platform, which connects blockchains *via* the Hub, and Polkadot, which uses relay chains to enable various chain interactions, have contributed significantly to the formation of blockchain chain networking. In the last 2 years, there has also emerged the cross-chain bridge Wormhol, the cross-chain liquidity protocol Coin9B, the decentralised cross-chain protocol Anyswap, and the Taylor public chain project that uses the POS liquidity mining mechanism to create a decentralised exchange to enable the interaction of assets on different chains. As a result, cross-chain technology has dramatically enhanced the performance of BT and promoted its widespread adoption. Cross-chain technology involves several issues, such as identifying, verifying, and processing data between chains. However, a secure cross-chain technology that applies to various scenarios and balances decentralisation and efficiency is still being explored.

In summary, after more than 10 years of development, blockchain has reliable theoretical guarantees and a wide range of application scenarios, and is now developing towards reliable and robust large-scale applications. Combined with the technological development of blockchain intergenerational and cross-chain interaction technologies, a blockchain system with grounded applications should have high performance, such as high scalability, throughput, high load and support for ultra-large-scale networks (Dang et al., 2019). However, the most significant technical bottleneck of the existing blockchain system is the low performance of interaction, which limits its application on the ground.

Based on this, the main contribution of this paper is to expound the research on the efficiency and data interaction of blockchain technology in different development stages, and to review the on-chain interaction technology, off-chain interaction technology and cross-chain interaction technology to improve the efficiency of blockchain. By combing the development context and route of blockchain high-performance interaction technology, this paper provides some guidance for researchers in the field of BT's efficiency in the future, and looks forward to the efficient application of blockchain in specific actual scenarios in the future.

In the setting of the chapter arrangement, this paper is divided into five chapters. The first section introduces the concept of blockchain and its current state of development, then describes the need to improve the performance of blockchain to meet the needs of large-scale practical applications. The following three sections analyse the on-chain interaction technology, off-chain

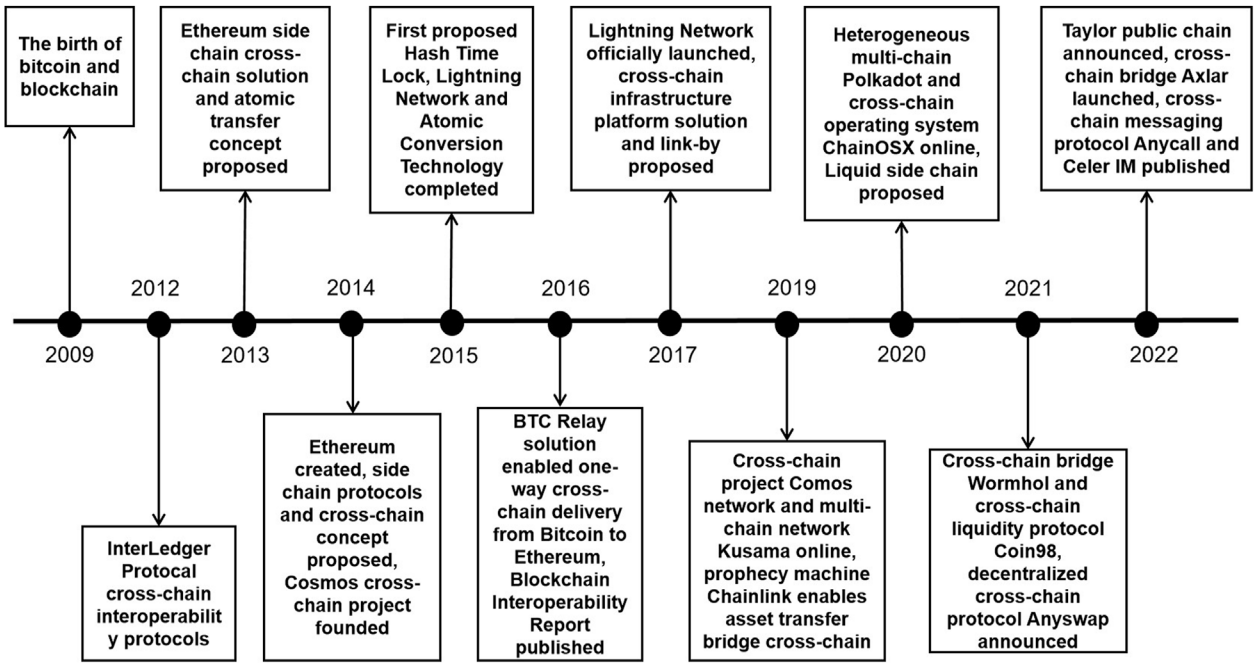

FIGURE 4
The development process of cross-chain technology.

interaction technology and cross-chain interaction technology of blockchain, respectively. The last section discusses the whole paper and gives an outlook.

2 High on-chain performance interaction blockchian technology

The blockchain industry is in the development stage, with many constraints in terms of technology and performance. Distributed storage architecture directly impact overall performance and flux, and blockchain performance-enhancing technologies to date have aimed to carry more transactions more consistently in a shorter period.

The finance industry is actively exploring the impact of transaction performance on both throughput and latency metrics, extends to various fields of academia and industry. Throughput represents the amount of transactions successfully processed by the blockchain per unit of time. Latency represents the transaction time it takes on the blockchain from being sent to complete processing. Currently, Bitcoin and Ethereum throughput are too low, supporting an average of 7 (Nakamoto, 2008) and 25 (Wood, 2014) transactions per second, respectively, far from meeting the needs of existing applications. In 2019, the Ethgasstation data site, based on the Ethereum network, became congested as network utilization soared to 90 percent, putting Ethereum at risk of losing existing users due to a lack of system scalability. Transaction latency can affect highly sensitive applications (Xu et al., 2021b) such as intelligent health systems, intelligent industries, and e-health services. Therefore, it must be improved as a low-latency and trusted blockchain system (Ejaz et al., 2021). There is no doubt that throughput and latency is affected by network bandwidth, making the blockchain network severely hampered by limited computing and bandwidth resources (Qiu et al., 2020). Therefore network bandwidth is also an essential factor. The performance of blockchain systems is inextricably linked to application scenarios. When faced with dynamically changing interactive information, such as in the field of energy systems, data throughput is significantly higher than in blockchain application scenarios for transaction settlement, which prevents the system from operating efficiently and even causes communication delays and message blocking (Liu et al., 2022a). In addition, throughput is closely related to the scalability and block capacity of the blockchain system. Scalability refers to relaxing the limits of each node on the blockchain involved in completing the processing and using a multi-layered processing architecture to spread the processing volume. Methods of blockchain improvement using this idea include Cross-chain, State Channel, Consensus Mechanism, Sharding, Partitioning, Side Chain, and other methods.

On-chain and off-chain technologies enhance performance through improvements to the structure of the blockchain system. The limited performance of the blockchain is enhanced by both on-chain scaling, which improves the basic mechanism of the blockchain, and off-chain scaling which extends additional architecture to improve the performance of the node network without changing the architecture of the blockchain system. The main factors governing blockchain scaling technology are divided into network load and node performance, which focus on the overall performance of the blockchain network and the performance of individual nodes, respectively. On-chain scaling mainly includes data, network, and consensus layer scaling solutions. The off-chain

scaling includes Side Chain, State Channel, Off-chain Computation, and other technologies. The scalability of a blockchain system is measured by throughput and latency, and the relevant technologies are improved based on these indicators to enhance the system's efficiency. Scaling the blockchain enables the system to handle a larger volume of transactions per second, reducing the speed of writing transactions into the system and thus shortening the time users wait for transactions to complete. The simulation system can be an effective tool for configuring high-performance blockchain systems. For example, the software BlockSim (Alharby and van Moorsel, 2020) simulates the dynamic system model by building the architecture layer of the blockchain to expand deployment details and performance impacts. Research on the blockchain scaling framework is divided into three parts: key technologies, constraints and derivative issues, and the technical elements and development directions of bitcoin scaling have been comprehensively examined, pointing out that bitcoin scaling has become a major trend under the close attention of various industries (et al., 2019).

The first cryptocurrency for blockchain applications, Bitcoin, has an average block generation time of 10 min in transaction processing, according to the blockchain.com website. In this case, the long time of generating block and the 1 MB block size limit forced researchers to improve their technology to increase performance and application scale. With the average block size of the blockchain steadily rising to 1.23 MB (Until 11 July 2022), the block capacity cap has been limiting this to users, and there is an urgent need for Bitcoin to scale. The on-chain scaling solution used to be the main scaling method with modifing and optimizing the basic protocol and architecture of the blockchain itself to achieve the scaling effect and improve system performance.

2.1 Data layer scaling

Architectural scaling solutions refer to the modification of the data block layer in the blockchain to increase the amount of transactions in the block itself. They are available in the following ways: Block Size increasing, Segregated Witness (SegWit), and the method of Directed Acyclic Graph (DAG).

2.1.1 Block size increasing

Expanding the block capacity can most directly increase the upper limit of block storage space size, with adding the amount of transactions the block can hold. This type of method is mainly focused on the field of Bitcoin. For example, Bitcoin forked out of BitCash from the original block size of 1MB–8 MB and 32MB, while another variant of BitcoinSV has a 128 MB block size (Wątorek et al., 2021). In smart contracts, the required gas replenishment limits the amount of gas consumed by a block and can be dynamically and carefully adjusted to real time network conditions to avoid transaction pile-ups or block wastage (Wenlin, 2020) Block scaling can be improved by arithmetic power, transaction volume, and dynamic adjustment. However, block size cannot be expanded uncontrollably due to the need for nodes to have effectively large amounts of block capacity information, which also increases the latency of block transmission in the chain and makes it more vulnerable to external attacks (Croman et al., 2016).

2.1.2 SegWit

SegWit is proposed to address transaction scalability by extracting the transaction signatures originally stored in the block and placing them outside so that more transaction records can be stored inside the block, thus indirectly expanding the block capacity. SegWit solves the problem of transaction extensibility by separating the digital signature, which takes up most of the space in the block, from the rest of the transaction information, and expanding the internal capacity of the block by making the digital signature invoked only at the authentication node (Lombrozo et al., 2015). The introduction and adoption of SegWit can help determine the total demand curve for Bitcoin transactions and maximize revenue when the adoption rate of SegWit is around 0.6 MB (Brown et al., 2021).

2.1.3 DAG

As a directed graph data structure that can start from any node and cannot be returned to that node through several edges, DAG changes the block-chain linear storage structure (Wang et al., 2022b). DAG is highly concurrent (Amen et al., 2022), i.e., each transaction can be submitted to a consensus as a separate "block." The consensus mechanism used by DAG allows the hash of the previous block to be passed according to rules, replacing the linear storage structure of a blockchain and increasing the throughput of the blockchain network. Although DAG dramatically improves the throughput of blockchain systems, it also suffers from double-spend attacks and high retrieval complexity (Deng et al., 2022). DAG allows each transaction to be booked independently, with no theoretical performance bottleneck but may introduce new security issues when the last transaction has to wait for a newly joined node to validate.

2.2 Network layer scaling

The concept of sharding comes from the traditional database idea of partitioning different rows of a data table into different partitions, keeping each shard on a separate database server instance to spread the load, or using sharding techniques to partition nodes and transactions (Wang et al., 2022a). The basic idea of sharding is to divide the nodes in the blockchain into several relatively independent shards, where a single shard handles smaller-scale transactions or even stores only part of the network state, and multiple shards handle transactions and deals in parallel, which will theoretically increase the throughput of the entire network (Jia et al., 2021). Applying deep reinforcement learning techniques to the sharding system and designing the optimal selection strategy for blockchain sharding by establishing a Markov decision process (et al., 2022c) can improve the throughput and scalability of blockchain processing transactions. While the transaction processing overhead across shards can hinder the upper limit of blockchain throughput, a study has designed an associative transaction allocation algorithm (Tao et al., 2022) to maximize the throughput of blockchain transaction processing and make the system stable and low error performance. Depending on the

sharding object, blockchain sharding is mainly network sharding, transaction sharding, and state sharding. Among them, network sharding is the foundation and state sharding is the bottleneck (et al., 2022a).

2.2.1 Network sharding

Network sharding divides the whole network into multiple sub-networks into different shards through a certain organization. Each shard processes part of the different transactions in the whole blockchain in parallel to complete the verification of multiple transactions simultaneously. Network sharding is considered one of the most important techniques to solve the blockchain scalability problem and improve blockchain performance (Huang et al., 2022), which can alleviate the uneven distribution of blockchain transactions to a certain extent. Nevertheless, there are still some challenges with the existing blockchain sharding algorithm (Guo and Yu, 2022). A large number of network shards makes the consensus security problem caused by containing fewer nodes inside each node. On the contrary, fewer network shards reduce the parallel transaction processing efficiency and make the network performance unable to meet the application requirements. Therefore, a reasonable choice of shard size is needed to balance security and network performance requirements. In addition, in blockchain networks based on the practical byzantine fault tolerance (PBFT) consensus algorithm (Xu et al., 2021c), the random distribution of malicious nodes can cause when the number of malicious nodes within a given shard exceeds one-third of all nodes in the shard, making individual shards unable to reach consensus on transactions and thus creating the problem of shard failure. To address these problems, specific algorithms can be used to make the dynamic evolution of the distribution of different types of nodes converge to a near-optimal equilibrium point, thus achieving a uniform distribution of nodes (et al., 2022d).

2.2.2 Transaction sharding

Based on network sharding, transaction sharding technology divides blockchain network-wide transactions into different network shards by rules for regional consensus. Different shards can process transactions in parallel, thus improving the overall throughput and performance of the blockchain system. The main transaction rules are the Unspent Transaction Output model and the Account/Balance model. The UTXO model means that the output of blockchain transactions that have not yet been spent can be used as input for new transactions, and the output of transactions that have been spent cannot be spent again and need to be transacted across shards (Liu et al., 2022c). The account/balance model means that the system records the balance of each account, and the system checks whether the account has sufficient balance for payment when a transaction is made. Multiple transactions for the same account can be guaranteed to be processed in the same shard as long as the transactions are shared according to the sender's address (Zhang et al., 2020). Blockchains based on a sharding scheme may have uneven transaction shards (Nguyen et al., 2019) and therefore need to be reasonably designed to allocate resources (Huang et al., 2022). For example, a nearest-fit correlated transaction allocation algorithm can select the shard with the closest remaining processing capacity to the amount of transactions in the transaction group and reasonably allocate transactions to different shards to improve blockchain throughput (Tao et al., 2022). In addition, sharding failure requires that transactions across shards be rolled back, which requires improvements to the validation scheme to reduce the rollback probability, increase the amount of transactions per second processed by the system, and create a larger sharding size (BAI Bing and LI, 2022).

2.2.3 State sharding

State sharding is achieved by distributing the storage of different parts of the ledger across the shards while the entire sharded network forms a complete ledger. This sharding approach relieves the pressure on each node to store information such as the ledger and reduces state storage redundancy. However, state sharding can make cross-shard transactions difficult to verify. Different sharding nodes need to transfer transactions or exchange the state of the ledger in some way due to their different stored ledgers (Sonnino et al., 2020). Although state sharding can essentially solve the blockchain performance scaling problem, there are high technical barriers that make it difficult to implement (Wang et al., 2019a). At the same time, blockchain state sharding transactions are randomly assigned rather than pre-planned, which can cause excessive transaction volume in a shard resulting in transaction blockage and overload. To address this problem, a multi-round verification node election scheme can improve the system's performance for transaction overload handling within a shard under state constraints while sacrificing latency to ensure security (QIN Wenhui and LI, 2021). Scalability and decentralized verification are made possible *via* state sharding. Ethereum, for instance, is split into 64 shard chains that are synced and independently recorded during the most recent Ethereum 2.0 upgrade event, which is particularly significant and well-known. It can considerably increase the system's efficiency, security, scalability, and speed (Guo and Yu, 2022). The 64 shard chains are required to produce blocks within 12 s, send verified block information and status data to the beacon chain, and pack them out of blocks under the Ethereum 2.0 system. The nodes in each partitioned chain will independently execute the consensus protocol and append blocks, and the smart contract will allocate transactions within performing transactional operations. Transactions between partitioned chains during cross-partition transactions will bypass the beacon chain and complete high-performance cross-partition transactional operations (Han et al., 2021).

2.3 Consensus layer scaling

The consensus layer mainly encapsulates the network nodes' various consensus algorithms, so the consensus layer's scaling solution is mainly to configure and optimize the consensus mechanism. A consensus mechanism is a set of rules that allows all participating nodes to agree on the outcome of a transaction in a blockchain network, ensuring that a decentralized blockchain system can make each transaction consistent and correct across all network nodes. The Consensus Mechanism aims to address the "Byzantine failures" (chuang et al., 2021), which is a consistency issue for distributed data systems, by creating a fair and effective method of managing nodes to reach a consensus on the design ethos.

There are three most representative consensus mechanisms: Proof of Work (PoW) (Nakamoto, 2008), Proof of Stake (PoS) (Larimer, 2013), and Practical Byzantine Fault Tolerance (PBFT)

(Castro and Liskov, 1999). The PoW obtains bookkeeping rights based on the workload of participating nodes. The PoS obtains the probability of bookkeeping rights based on the monetary value and time allocation owned by participating nodes. The PBFT is a class of state-machine Byzantine protocol that replicates copies at different nodes in a blockchain distributed system so that each copy takes consistent actions to maintain the state of the service and implement operations. It also includes a variety of consensus algorithms, such as hybrid consensus mechanisms, to reduce the time it takes for the system to reach consensus, thereby improving system performance. However, PoW is relatively secure but not conducive to performance scaling, Pos-type consensus mechanisms tend to form monopolies, and BFT-type consensus has strong consistency but is limited by bandwidth and number of nodes, resulting in significant performance degradation.

In the Ethereum 2.0 upgrade, switching to the PoS consensus protocol from the PoW protocol will enable the Ethereum blockchain system to use less energy in terms of arithmetic power, conserving energy while creating a more elaborate network architecture (Alvi et al., 2022) that can achieve a TPS of 100,000 (Khoury et al., 2022). In Proof of Stake, different nodes store only part of the data, and the elected committee is responsible for voting to verify the blocks. Each transaction is only verified locally within the shard instead of being passed to the whole network for verification, achieving the goal of saving network-wide bandwidth and improving overall system throughput. The PoS consensus on Ethereum 2.0 is handled by the consensus layer of the ETH 2.0 Client, which implements the mechanism in the Beacon Chain nodes and enables each participating node to register and pledge. The beacon chain is used for transactions and transfers. By merging with the Ethereum main network, it marks that the consensus protocol of Ethereum has been completely converted to PoS. If the consensus protocol is not followed, the stakes of participating nodes will be reduced so that the system's fairness will be guaranteed by the beacon chain. PoS also randomly allocates shards to verifiers, allowing verifying nodes to pledge Ether and pass information through an asynchronous cross-domain architecture model on the beacon chain, improving the security of the shards and the overall system (Cassez et al., 2022).

The Red Belly Blockchain is recognized as the first secure blockchain that uses lateral expansion features, allowing throughput to scale to hundreds of geographically distributed consensus participants and revisits the BFT class of blockchains from three perspectives on this blockchain system: Byzantine consensus mechanisms, leaderless design, and sharding (Crain et al., 2021). Compared to other consensus mechanisms, PBFT is more suitable for partially decentralized, anti-Byzantine consortium chains with a strong consistency of nodes. However, PBFT is limited in the size of networks it can support (Chen et al., 2022). Through a blockchain digital asset platform with multi-party authentication functions, verifiable BFTs are embedded for randomly selecting consensus nodes in the supply chain to improve node security (Liu et al., 2022b). Also, achieving node consistency in a distributed system is complex as it requires consistency mechanisms to maintain adversity tolerance, fault resilience, partitioning across the network, delay persistence, security measures and other important properties (Lashkari and Musilek, 2021). The Blockchain Trilemma has always been a challenge in its technology, i.e., security, decentralization, and scalability cannot exist simultaneously, as shown in Figure 5.

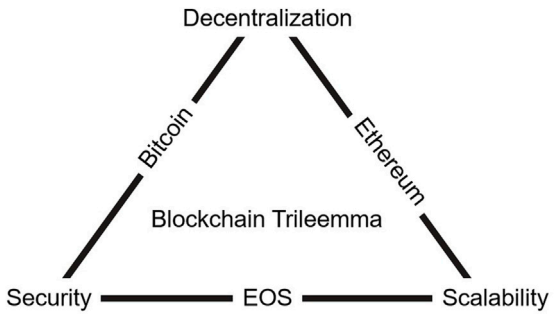

FIGURE 5
The blockchain trilemma of BT.

The three attributes of a blockchain cannot be satisfied at the same time, so there are trade-offs and dynamic planning. The Monoxide model, a high-performance blockchain system proposed by Dr. Jia-Ping Wang (Wang, 2022) of the Institute of Computing, Chinese Academy of Sciences, can simultaneously satisfy the triangular characteristics of security, high performance, and decentralization by using asynchronous consensus zones with minimal introduction of additional entities and mechanisms, enabling the blockchain to scale horizontally by more than 1,000 times, thus increasing data throughput by more than 1,000 times. Asynchronous consensus is not necessary to reach consensus immediately after each block is generated, but each node does its best to produce a block while following the asynchronous graph algorithm and reaches agreement after a period of time. The literature (Wang and Wang, 2019) achieves asynchronous consensus by running multiple independent and parallel regions of a single-chain consensus system and proposes eventual atomicity to ensure transactional atomicity of the regions. Consensus mechanisms for distributed systems will be a difficult and hot research topic for blockchain systems for a long time (et al., 2020b).

Additionally, BT raises some privacy and security concerns for users due to its data traceability, the openness of transactions, and the continual development of analytics. Therefore, balancing privacy in BT is also a major issue. In Bitcoin and Ethereum systems, transaction data information is open and transparent to anyone, which makes it possible to reverse the identification of users based on relevant information. This traceability and linkability weakens the anonymity of blockchain systems and poses a potential risk of user information leakage (Ermilov et al., 2017; Fröwis et al., 2020). In terms of improving anonymity, Monero (Van Saberhagen, 2013)has achieved strong anonymity of blockchain systems by solving three major linkability problems, traceability, and hiding the amount of money (Pedersen, 1991)through three techniques: one-time addresses, ring signatures (Fujisaki and Suzuki, 2007), and Ring Confidential Transactions (RCTs), respectively, which have won market recognition. Meanwhile, the Monero team has continuously updated these three technologies (Liu et al., 2004). Firstly, in 2018, a non-interactive zero-knowledge proof mechanism called Bulletproof was integrated into the protocol, resulting in a

significant reduction in transaction capacity and fees per transaction. Secondly, in 2020, the ring signature technology was upgraded with a concise linkable spontaneous anonymity group CLSAG (Concise Linkable Spontaneous Anonymous Group) signature scheme, which further reduces the transaction size and verification speed and improves the operational efficiency of the system. Currently, Monero's TPS can reach 1700, which already meets most nodes' needs. However, compared with the 100,000 TPS of the upgraded version of Ethereum 2.0, which replaces the POW protocol with the POS protocol, its operation efficiency still seems low. This shows that BT's trade-off between privacy security and efficiency is still worth considering.

In general,on-chain scaling allows blockchains to scale with more flexible systems and larger block sizes, thus allowing blockchain networks to scale to larger transaction volumes in real-time. However, as all transactions still need to be synchronized in the distributed system of the blockchain, the performance bottleneck of the entire network will depend on the processing performance of individual servers. The online scaling programme still needs to work on the implementation and deployment side. It is worth noting that larger capacity blocks will impose higher costs on nodes and bandwidth, reducing the proportion of nodes with slightly less processing power and increasing centralization.

3 High off-chain performance interaction blockchian technology

Nowadays, with the maturity of scaling technology, it is widely believed that on-chain scaling solutions can have an insurmountable ceiling in terms of performance (Hepp et al., 2018). Storing data off-chain can save the data occupied space and computing resources on the chain, and can also adopt corresponding technologies to ensure the privacy and security of data. The off-chain data storage method mainly includes smart contracts. Under the condition that technologies such as knowledge graphs are used to ensure data sharing and encryption, the blockchain framework is optimized to achieve high throughput of parallel processing (Yao et al., 2021). The main idea of off-chain scaling is to transfer part of the data to the off-chain for computational processing and return the final result to the on-chain for storage and recording. Depending on the various modes of data transfering, there are currently two main technical routes: State Channel and Off-chain Computation. The interaction between on-chain and off-chain data can be carried out through cross-chain technology.

3.1 State channel

A state channel is essentially an account created on the main chain that is jointly controlled by multiple nodes, with the aim of transferring a large amount of computation in the blockchain to be performed off-chain, and can effectively address the large number of high frequency and small transactions that currently exist. This technology allows for a large amount of interactions not to be broadcast across the blockchain, but only between the participating nodes, with the transfer being mainly off-chain channel interactions and on-chain clearing. The participants of the state channel are limited to business-related parties, which avoids data privacy leakage to unrelated nodes, provides better security, and can close the channel and update the state at any time, which is especially suitable for scenarios with high frequency data interaction between fixed parties.

The general process for using State Channel is: locking the state, opening the channel, data interaction within the channel, closing the channel, submitting the updated state, and clearing the chain (et al., 2020b). Data interaction and state updates within the channel are without blockchain system consensus, and many transactions are conducted off-chain, which can significantly enhance the transaction throughput of the blockchain system (Qiwu, 2020). The Lightning Network enables participants to make frequent two-way payments *via* two-way channels under the chain. In contrast, the literature (Pan et al., 2019) proposes the first multi-way payment channel scheme. When a smart contract receives a deposit from a participant, frequent transactions can be made between multiple parties within the channel without having to go through cross-channel payments. The literature also addresses the problem of an excessive number of channels and inefficient routing algorithms that exist in two-way payment channels such as lightning networks.

3.2 Off-chain computation

The idea of off-chain computation is to put complex transactions off-chain for execution and then submit the results of the transaction structure back to the chain, with the chain only verifying the data, thus indirectly improving the speed of blockchain processing transactions. The main solutions for off-chain computation include Trusted Execution Environment (TEE) computation, Secure Multi-Party Computation (SMPC), and Incentive-driven Off-chain Computing (IOC).

3.2.1 Trusted execution environment

An environment where off-chain computation is executed in a TEE so that certain types of nodes running transactions are necessarily reliable and cannot be modified by outsiders. This engineering solution was originally used for privacy computing, based on hardware to create a black box-like environment. Therefore, the privacy of blockchain systems can also be secured with the help of machine learning or related software that performs many complex operations in the execution environment. Once privacy AI technologies such as federal learning and TEE are integrated with blockchain, they will have strong error correction and compound interest generation capabilities (Passerat-Palmbach et al., 2020). A TEE can enhance the security benefits of multiple operations on blockchain privacy protection to a certain extent. However, it is difficult to apply on a large scale due to the highly demanding hardware environment. To achieve fine-grained privacy protection for decentralized applications, the throughput and performance of blockchain systems can be enhanced by utilizing *ad hoc* processing of privacy data while enabling on-chain execution of public data processing *versus* off-chain execution of privacy data processing (et al., 2020a).

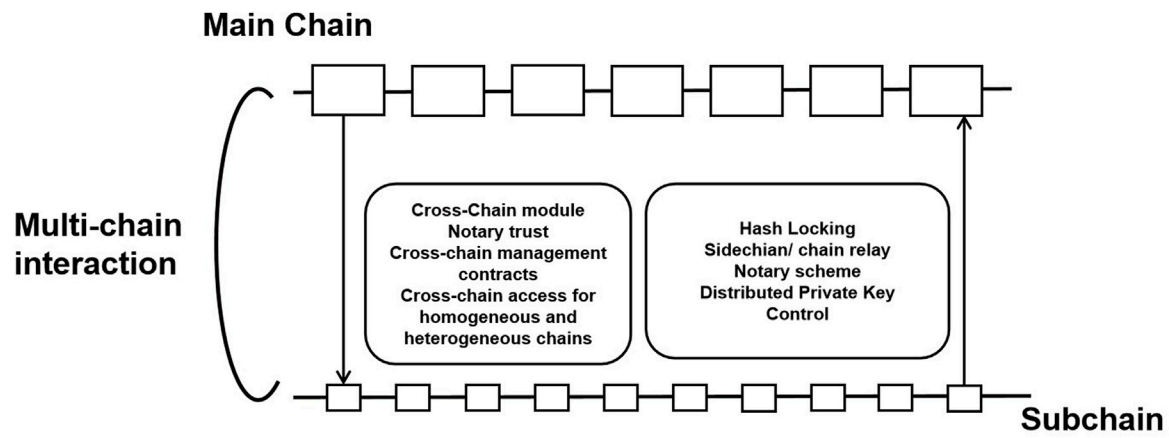

FIGURE 6
Blockchain overall cross-chain architecture.

3.2.2 Secure multi-party computation

Off-chain computing enables an application approach where data is available and invisible through secure multi-party computation, providing software algorithm-based encryption compared to TEE. This software and algorithmic theory enable data to be both private and usable, combining blockchain features to enable user data privacy to be secured, thus unlocking the immense value of private data sharing, data analysis, and data mining (Wang et al., 2019b). The off-chain secure multi-party computation first locks the public state on the chain, then distributes the data to the off-chain for secure multi-party computation, and finally combines the results of each computation and returns them to the chain for verification. Considering the limited space capacity of the blockchain, it is possible to put the privacy calculation and Secure Multi-Party Computation of a large amount of data into the off-chain operation and then use the channel to make the data information interchangeable, thus improving the on-chain performance and processing speed. Integrating private messages into blockchain networks by combining different anonymous valid signatures can provide a new approach to secure multi-party computing for secure and efficient data privacy protection, reducing the overhead of significant computation time and storage (Feng et al., 2021b). Several projects have experimented with secure multi-party computing protocols such as Defi, Enigma, etc. Enigma is an effective solution to private data processing by allowing servers to use secure multi-party computing to run computations in a distributed manner directly on the network without the server being able to observe the original data (Xie et al., 2019).

3.2.3 Incentive-driven off-chain computing

The method of IOC uses an incentive mechanism to motivate the participants, assuming they are ideal economic agents, to handle the computational task and check the correctness of the results. These two steps are performed by a solver and a verifier located below the chain, respectively, with the solver being rewarded if the calculation is correct and penalized otherwise. The main off-chain projects deployed and run as incentive-driven models are Truebit(Teutsch and Reitwießner, 2019), a technology that helps Ethereum perform heavy or complex calculations offline (Stark, 2018). The basic principle is that users request a calculation and pay a commission. A solver under the chain provides a deposit to perform the calculation simultaneously and publishes the result. A verifier provides a deposit to rerun the above calculation and check if the solver's result is incorrect. If successful, the solver is offered a commission. If not, a challenge can be launched and submitted to the chain for arbitration.

SegWit technology is the basis for off-chain scaling and can be attached to on-chain scaling. The full deployment of witness segregation-based Lightning Network technology can significantly increase transaction processing capacity and reduce confirmation times. Thus off-chain scaling can reach nearly unlimited transaction processing capacity, but the network takes time to build (YU Hui and Zhang, 2017). The State Channel and Side Chain in the off-chain scaling solution are derived from improving new technologies to Bitcoin and Ethereum's flaws and have been validated by more projects and gradually promoted. In contrast, the Off-chain computation solution has less implementation validation than the former. The off-chain scaling still needs to deal with latency and security issues. It takes a transitional development period to achieve the theoretical results and still has great room for development.

4 High cross-chain performance interaction blockchian technology

In addition to on-chain technology, cross-chain technology is also regarded as an important way to improve the efficiency of blockchain interaction. On the one hand, cross-chain technology can realize the connection between different blockchains and realize the functions of information interaction and value transfer to form a chain network (Tam Vo et al., 2018) and achieve the purpose of interconnection (Li et al., 2019). On the other hand, through cross-chain technology, transactions can be transferred, thus enhancing the efficiency of data processing. The development of cross-chain technology is driven by the demand at the time of blockchain application, from the initial demand of mining and financial

transactions, gradually transitioning to multi-industry applications, and now to the era of chain networking, where the increasingly high performance and interaction requirements have prompted the creation of more and more cross-chain technologies (Cai et al., 2019). Cross-chain interoperability makes large-scale blockchain applications possible, driving the entire industry forward.

4.1 Key issues in cross-chain technology

The data on the blockchain is up or down by the consensus mechanism designed by the blockchain itself (Nofer et al., 2017), after which it is stored on all end nodes, and all full data nodes form a distributed cluster in a way that makes transaction data tamper-proof (Yaga et al., 2019). On the one hand, this enhances the security of the data, but on the other hand, it makes each chain relatively closed and inevitably poses problems when interacting. From the current practical application of cross-chain technology, it is crucial to consider the problems in the three phases of start, process, and result when interacting with data between different chains.

4.1.1 Authenticity of initial information

The blockchain itself is still a relatively closed system. Information on one chain is external to another chain, and it is an important question to ensure that this external information is correct and final when it enters the other chain. The simplest solution to the current problem of chain-to-chain access to information about each other is to have multiple nodes listen to contract events on the blockchain simultaneously. When the vast majority of nodes agree that they have seen the event, it can be assumed that there is a consensus between the nodes to trigger the next event in the sequence. BT can ensure that information is immutable and always trustworthy during the flow (Golosova and Romanovs, 2018). However, the authenticity of information at its most source needs to be ensured collaboratively using other mechanisms. This is the key to many cross-chain technologies, namely, the verification and delivery of information.

4.1.2 Transaction atomicity

Transaction atomicity (Collado et al., 2013)means that transactions are treated as a whole and contain processing actions that either succeed or all fail, rather than partial successes and partial failures. Once a transaction is successful, subsequent cross-chain or non-cross-chain transactions can proceed normally; if a transaction fails, the current transaction can be rolled back or reversed without affecting future transactions. The concept of transaction atomicity was first introduced in hash-locking technology, where the inability to guarantee atomicity could lead to double-spending (Karame et al., 2012).

4.1.3 Transaction consistency

The state of the chains before and after a transaction is executed on both chains is consistent, meaning that things can be executed correctly (Belchior et al., 2021; Zhuoyan and Xuan, 2021). For example, if a user on chain A transfers 100 bitcoins to a user on chain B, then the user on chain B should get 100 bitcoins. If the user on chain B only gets the equivalent of 70 bitcoins, then the state of both chains needs to be rolled back. This requires feedback and validation of the outcome and status of cross-chain transactions, guaranteeing that the sum of the assets on both chains remains the same in the case of asset transfers or that the amount of assets on each chain remains the same in the case of asset exchanges.

In addition to these three issues, there are other cross-chaining issues, such as the security issues that come with cross-chaining. Some large cross-chain platforms nowadays usually have many different chains interacting with each other. If a security issue arises in one chain, can it be isolated quickly to prevent the impact on other chains within the platform? In addition, as the interaction deepens and the number of interacting chains increases, can the transaction performance be supported? The management issues and user data privacy (Liao et al., 2016; Eyal and Sirer, 2014; Holbrook, 2020; Feng et al., 2021b) for cross-chains are also hot topics.

4.2 Mainstream cross-chain technologies

Many technologies (shown in Table 1) try to overcome the difficulties of cross-chain technology and exploit the synergies of the chain (F et al., 2019). For homogeneous chains with the same underlying logic, topology, consensus mechanism, block generation logic, etc., cross-chain technology is relatively simple, and the interaction mechanism can generally be built directly. For heterogeneous chains with significant differences, it is more difficult to build the interaction mechanism directly, and the cross-chain effect is usually needed with the help of a third party. Then the design of the third party is also the important point. Currently, there are four main cross-chain schemes, notary scheme, side chain and chain relay,hash-locking and distributed private key control (shown in Figure 6). These cross-chain models have also led to the creation of many cross-chain platforms, such as Interledger (Thomas and Schwartz, 2015), which implements different types of ledger connection and operation models with mainly notary schemes; the sidechain/relays projects represented by Pegged Sidechains (Poon and Buterin, 2017; Kwon and Buchman, 2016), which provide different cross-chain network platforms; and projects based on hash lock (Poon and Dryja, 2016), in which the feasibility of the technology has been verified several times. To a certain extent, these technologies have solved the interoperability of information, assets and functions between different chains, extended the development space of BT and promoted the improvement of the networking of value blockchain chains.

4.2.1 Notary scheme

The notary scheme (Bingrong et al., 2021)is a cross-chain mechanism that is relatively easy to implement. In simple terms, when two different chains want to interact, a trusted third party can assist in verifying and forwarding the information across the chains. The third party under this mechanism has accounts on both chains. The trusted third party can automatically or request to listen for events on the different chains, use a specific algorithm to determine the validity of the events and other issues, and then respond with follow-up action. This third party acts like an intermediary, and the process can be likened to the operation of foreign exchange in life, where a foreign exchange bureau acts as a trusted third party. The rest of the different subjects exchange national currencies freely through the bureau.

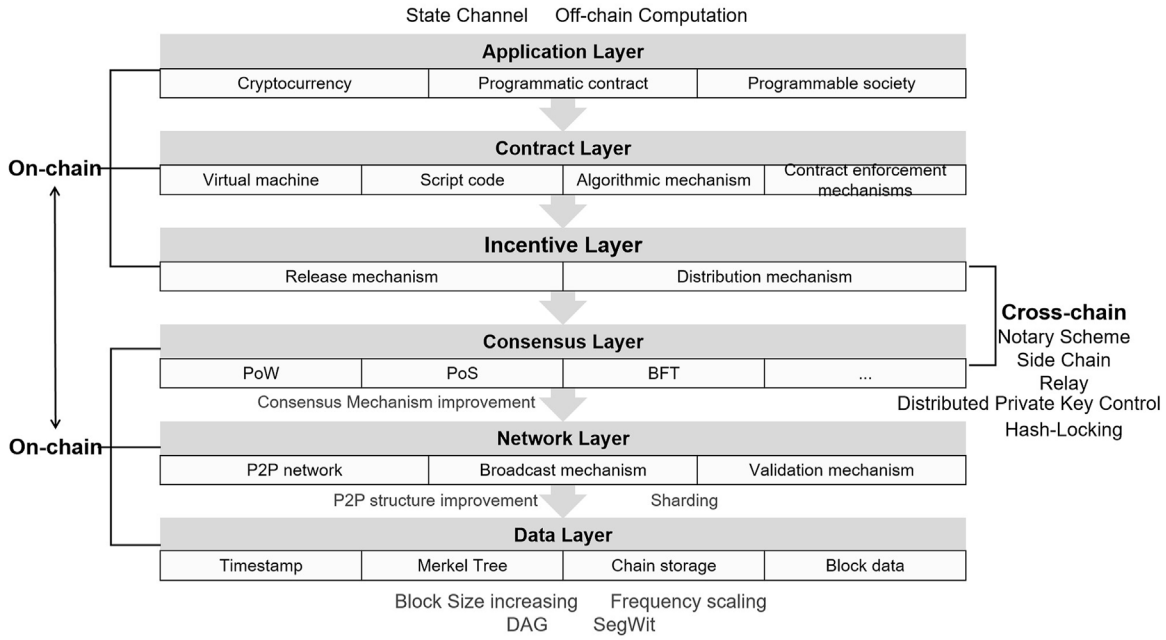

FIGURE 7
Blockchain architecture diagram.

Currently, the number of notary nodes in the implementation of notary scheme and the difference in signature methods can be divided into single-signature notary scheme, multi-signature notary scheme, and distributed signature notary scheme. A single-signature notary scheme, also known as a centralized notary scheme, is a simple and efficient way to act as a notary through a single independent node or institution but faces the problems of high centralization and security vulnerabilities. A multi-signature notary scheme selects a random number of notaries for each transaction confirmation, each with a key, and only a certain percentage of notaries sign the transaction before it occurs, which is more secure than a single-signature notary scheme (Rivest et al., 1978). The distributed signature notary scheme uses multi-party computation (MPC) technology to achieve its security (Chaofan et al., 2021; Feng et al., 2021c; Liu et al., 2022b), splitting the key into multiple parts and sending it to the notary at random, which is the most complex and secure of the three types.

4.2.2 Side chain and chain relay

Side chain and Chain Relay (Gaži et al., 2019; Frauenthaler et al., 2020b)are one of the most commonly used cross-chain mechanisms in the market today and require collecting information from the original chain in the process. In contrast to the notary scheme described above, this scheme can verify the transaction data itself, eliminating the risk of an inevitable centralization of the notary scheme, while the scheme expands the extensibility through various interfaces. The concept of side chain first appeared in Bitcoin. It was used for various forms of bookkeeping with interoperability between distributed systems, aiming to extend the functionality of the Bitcoin protocol layer (Back et al., 2014). Side chain is relative to the main chain, and the link between the main chain and side chain is implemented based on two-way peg technology. With a two-way peg, the master and side chain can lock and release assets on each other's chain for asset transfer. It can help the master chain handle transactions. Once too many transactions are on the main chain, and a performance bottleneck occurs, the assets and transactions on the main chain can be transferred to the side chain for processing by transferring them to the side chain. This reduces the pressure on the main chain and achieves the purpose of extending the functionality and performance of the main chain (Back et al., 2014), which is currently an important method to improve the interactive performance of the blockchain.

A relay chain, also known as a relay, builds an operational channel between different chains, provides a unified cross-chain communication protocol, and connects other blockchains for interconnection by only collecting the data state between the two chains through the relay chain for verification.

Side chain and Chain Relay cross-chain model allows for the creation of a smart contract in the chain that takes the block header of the originating chain as input and uses standard checks within the originating chain to verify that the blockchain meets the consensus algorithm specification requirements. Side chains/Relays is based on light-client verification technology, where a smart contract with blockchain-like light-client functionality is executed on one chain during a cross-chain interaction, verifying that a particular transaction, event, or state information has occurred between the chains *via* the cryptographic hash tree of the other chain and the block header (Frauenthaler et al., 2020a).

4.2.3 Hash-Locking

Hash-Locking (Kang et al., 2007; Dai et al., 2020; Feng et al., 2021a), known as the Hash time lock contract, is a cross-chain

TABLE 1 Comparison of mainstream cross-chain technologies.

Property	Notary scheme	Sidechain and relay	Hash-locking	Distributed private key control
Representative Project	Interledger/Croda	Cosmo/Polkadot	Lightning Network	Wanchain/Fusion
Interoperability	Transaction type set by the notary	Transactions (transfers and contract calls)	Transaction of transfer type	Transaction of transfer type
Transaction Speed	Slow	Medium	Slow	Medium
Trust Model	Majority consistent of notaries	Against the 51% attack	against the 51% attack	against the 51% attack
Cross-chain Asset Transfer	Support (requires long-term notary signature)	Support	Not Support	Support
Cross-chain Primitives	Support	Support	Not support direcly	Support
Cross-chain Asset Mortgage	Support (requires long-term notary signature)	Support	Mostly supported with some difficulty	Support
Multi-currency Smart Contracts	Difficult	Difficult	Not support	Support
Implement Difficult	Medium	Difficult	Easy	Medium
Atomicity	Notary Guarantee	Contract Implementation	Hash Lock/Timeout Mechanism	Multi-signature Algorithm
Generality	Platform type set by the notary	Platform type set by the side chain or relay	Lightning Network supports Bitcoin	Support script mechanism and Signature verification
			Raiden Network supports Ethereum	mainstream public chain, Consortium chain
Security	Low (Notary Mutual Trust Mechanism)	Medium (Merkle Proof)	Low (Hash Algorithm)	Medium (Multi-Signature Algorithm)
Scalability	Slightly Extensive (Notary Decisions)	Limmited (Parallel Scaling)	Extensive (Parallel Scaling)	Limmited (Parallel Scaling)

technology solution to exchange assets between chains using a hash lock and a time lock. In this scheme, the participation of a third-party trusted notary is not required. Both parties unlock assets locked in smart contracts on different chains by passing hash proxies and hash values while setting their time locks to ensure that the operation time enables atomic operations to exchange assets. This solution can either facilitate the transaction or make it abandoned. The atomic swap protocol of hash locking ensures that the total amount of assets in the same chain remains unchanged. Still, at the same time, the use of hash locking is limited and can usually only be used for cross-chain asset exchange and does not enable the cross-chain transfer of assets. Hash locking is widely used in the technical architecture of the Lightning Network, which is essentially a mechanism for securely performing zero-confirmation transactions using hash-time-locked smart contracts. At the same time, time-locked contracts provide a good middle ground between accuracy and sensitivity for Lightning Networks (Nowostawski and Tøn, 2019). In recent years, the scheme has also been improved, and a cross-chain asset interaction protocol based on an improved hash time lock has been proposed. It achieves secure and seamless asset transformation between Ethereum and consortium chain networks and considers atomicity, fairness, and transparency (et al., 2022b).

4.2.4 Distributed private key control

Distributed private key control technology is based on a distributed key distribution mechanism, similar to the distributed signature notary scheme, but can further avoid the risk of centralization. Distributed private key control technology introduces the ability to lock and unlock digital assets in a mutually reversible manner, separating the use and ownership of digital assets and thus managing and manipulating the tokens on the original blockchain. Based on blockchain protocols with built-in asset templates, new smart contracts are deployed to create new cryptocurrency assets based on cross-chain transaction information, thus mapping digital assets from multiple different blockchains onto a new blockchain and enabling digital asset exchange (Patin, 2019) between different chains on this new blockchain.

The differences between the cross-chain schemes lie mainly in how these three steps are implemented. The main differences are in the transmission channels and the authentication methods, so they have a different emphasis. As the value of blockchain is continuously explored, there will be more and more various blockchains in the future, and the cross-chain technology connecting different blockchains will also become more critical. Choosing the right cross-chain technology under different scenarios and needs is the key to realizing the value transfer and information interaction between chains.

4.3 Comparison of mainstream cross-chain schemes

Currently, cross-chain technology still has many shortcomings, and it is difficult for one cross-chain technology to consider various

TABLE 2 Summary of high-performance data interaction technologies.

Category	Programmes	Layers	Technologies	Representative	Advantages	Shortages
On-chain	Block Size increasing	Data Layer	iexpand space within the block	BIP100-109	easy and instant	bifurcating
	SegWit	Data Layer	place signatures off-chain, save on-chain space	BIP141	safe and low cost	bifurcating and limit expandable
	DAG	Data Layer	change storage structure to directed concurrency	IOTA	relate nodes with transaction speed	lack formula proof
	Consensus Mechanism	Consensus Layer	improve or hybrid use of consensus protocols	high or hybrid PoW,PoS,BFT	improve efficiency and low energy	limit consensus protocols
	Sharding	Netwok Layer	node segmentation and concurrent processing	Zilliqa	parallel and fast processing	complex cross-shard communication
Off-chain	Off-chain Computation	Layers of Incentive, Contract Application	execute transactions off-chain and audit on chain	Defi, Enigma,Truebit	sufficient theoretical support	delays and side chain risk
	State Channel	Layers of Incentive, Contract, Application	create a private channel for two-way data interaction	Perun, Egger	ensure data privacy and real time	hard to support large transaction
Cross-chain	Notary Scheme	Layers of Incentive, Contract Application	validate transaction information through third-party	Interledger	simple, support heterogeneous chains	limit third party notaries
	Sidechain and Relay	Layers of Incentive, Contract Application	operability and exchange between main and side chains	Plasma, Cosmos	easy implement and apply, usable	hard to storage data and develop
	Hash-locking	Layers of Incentive, Contract Application	time setting and mechanism based on atomic exchange	LightningNetwork, NCASP	improve decentralization and security	complex operation, inflexible
	Distributed Private Key Control	Layers of Incentive, Contract Application	reversible operations for locking and unlocking, distribution	Fusion, Wanchain	avoiding SPOF and decentralized	hard to develop, time-consuming

scenario uses. The challenge of next-generation cross-chain technology is to satisfy the five aspects of capital efficiency, security, scalability, statefulness, and speed (F et al., 2019). A comprehensive comparison of the current mainstream cross-chain technologies is shown below.

4.3.1 Notary scheme

The notary scheme is a scheme that uses a third-party intermediary to implement cross-chain. A trusted third party is responsible for verifying cross-chain information and packetizing and forwarding transactions to both parties' chains. This cross-chain scheme is simple and convenient and can flexibly support a variety of blockchains with different structures for cross-chain operations, provided that the notary has access to the relevant parties' on-chain information. However, the disadvantages are also more apparent. Although multiple signatures reduce the risk of centralization, there is still the possibility that the notary may modify the cross-chain information and cannot be completely decentralized, which conflicts with the essence of blockchain.

4.3.2 Side chain and chain relay

The advantage of the side chain scheme is that it is simpler to implement, has more application scenarios, and can also improve the efficiency of blockchain interaction; the relay mode can be applied to the interlinking of homogeneous and heterogeneous chains, and different chains can be connected to relay chains, which is a more direct way to achieve interoperability. Relay chains can essentially be seen as a fusion and extension of the notary and side chain scheme. Although it can negatively affect the degree of decentralization of the blockchain network and hinder the decentralization of the blockchain network to a certain extent (Shahsavari et al., 2022), in contrast, it is not as risky of centralization as the notary scheme. Relay methods support functions such as cross-chain asset exchange, collateralization, and cross-chain contract implementation and are relatively rich in application scenarios. In terms of security, for the side chains scheme, if the main chain is hacked or compromised, the side chain can still operate, while a cyber attack on the side chain will not affect the operation of the main chain (Uddin et al., 2021). However, it is also important to note that side chains increase the complexity of the network and assets, which can expose the system to the risk of new attack vectors and centralized mining (Gudgeon et al., 2020); for the relay scheme, the security of relay and parallel chains are affected by each other, and when a security incident occurs in one parallel chain within the network, there is uncertainty about the security of other parallel chains. In addition, the implementation of relaying across chains is complex and more difficult to develop. In the case of Polkadot, for example, the cumbersome way the various chains are connected is one of the key reasons why the project has been unable to make a huge breakthrough. In addition, relaying requires that

each blockhead of the target blockchain be stored by the target blockchain, which can entail expensive operational costs.

4.3.3 Hash-Locking

The hash locking technology originated from the Lightning Network uses the atomic exchange to achieve cross-chain, which can guarantee the authenticity of the information. However, using hash locking requires the construction of multiple transactions, which is complicated to operate (Herlihy, 2018). In addition, there are other disadvantages as well, one of which is that it is only applicable to the exchange of assets and not to the transfer of assets, making it much less applicable. The other is that there is a time lag in the transfer of assets, which can make it unfair to the other party that the initiator of the transaction has the power to decide whether or not to trade and thus break the contract under unfavorable conditions (Xu et al., 2021a). The scheme also requires the two chains to parse the contractual data between parties, such as asset locking data, which would require a high level of technology. In addition, if a peer-to-peer counterparty cannot be found, it must wait and is, therefore, less efficient.

4.3.4 Distributed private key control

The advantage of distributed private key technology is that the private key is kept by multiple nodes, reducing the negative impact of a failure at a single point on the whole. At the same time, it uses multi-party computation in cryptography and threshold signature techniques to, to a certain extent, avoid the risk of centralization under the notary mechanism. Distributed private key control technology can be applied to the interaction between various chains and can complete transactions without changing the chain, which makes its application scope wider in theory. However, on the other hand, its strict technology also raises the complexity of smart contracts. It increases the difficulty of contract development, while the cumbersome verification means increases the transaction time and reduces the transaction speed, which will be detrimental to some instant transaction scenarios with high requirements for transaction time. This will be detrimental to some immediate trading scenarios that require high transaction length.

Most blockchain systems lack interoperability features at their inception, and cross-chain technologies need to be designed and implemented with a focus on how to adapt to various types of blockchains and ensure efficient and highly secure cross-chain operations (Li et al., 2019). The existence of cross-chain technology and cross-chain platforms currently enables the interaction of assets and information between different blockchain systems to a certain extent, better leveraging the value of BT. However, at the same time, a comparison of the four mainstream cross-chain schemes reveals that the different schemes still do not strike a good balance between transaction speed, decentralization and extensibility. There are still deficiencies in block link entry rules, cross-chain protocols, identity management, etc., which makes no single technology able to meet the needs of all application scenarios and application populations. The value of BT can only be fully utilized if different technologies are used according to the needs of different scenarios and people.

5 Conclusion and outlook

How to effectively solve the high-performance data interaction problem of blockchain is the cornerstone to supporting the implementation and deployment of large-scale applications, providing low-latency and high-throughput technology support for programmable society and smart contracts. In this paper, the core of the blockchain high-performance data interaction technology is reviewed and analyzed from three perspectives: on-chain interaction technology, off-chain interaction technology, and cross-chain interaction technology. This paper concludes that the solution to high-performance data interaction technology cannot rely solely on a breakthrough in one or a few critical technologies in the blockchain and its architecture but should be considered within the overall six-layer system architecture (YUAN Yong, 2016) of the blockchain, as shown in Figure 7.

It should focus on the on-chain performance improvement of the data layer, network layer, and consensus layer, combine with the relevant off-chain computation advantages, use the state channel to transfer part of the on-chain low-performance processing data to the off-chain, and finally use various cross-chain technologies to break the bottleneck of the single-chain and improve the overall blockchain architecture performance. The differences between different solutions mainly lie in the different ways of implementing these three steps, among which the most significant differences are reflected in the different transmission channels and validation methods; thus, their focus also differs. The details are summarized in Table 2.

As seen in Table 2, on-chain scaling technology solutions are limited mainly by the number of nodes and transactions in the network, with limited performance improvement and bottlenecks in development due to the Blockchain Trilemma. Unlike on-chain scaling solutions, which modify the blockchain architecture, off-chain scaling techniques transfer complex computations and high-frequency transactions off-chain and store only the final results on-chain. However, off-chain scaling faces issues such as nodes going offline, transaction size, and deposit locking. In addition, the security of off-chain calculations, the verification of results of complex calculations, and the support for complex operations (such as smart contract invocation) are challenges that need to be addressed by off-chain scaling technology solutions. In terms of cross-chain technology, no cross-chain mechanism can effectively solve various problems and apply them to various scenarios. Therefore, considering the different focus of different cross-chain technologies, we can look at the following two aspects and six points.

5.1 In terms of on-chain and off-chain scaling technology

Currently, the on-chain scaling technology is considered to have reached a performance bottleneck and cannot cope with application scenarios that demand higher performance. At the same time, the established underlying protocols in the blockchain system cannot be changed much, making it impossible to make a breakthrough in the short term in terms of block size increase and consensus protocol improvements in on-chain scaling solutions. Consensus protocols can build the technical mechanism of cryptocurrency and create

their asset value in the market, which can be used to stabilize the overall price. DAG technology and state sharding, which change the storage structure of the blockchain, require a high level of technical implementation and need further improvement in implementation and deployment.

Although the off-chain scaling technology does not improve the system's performance from blockchain, it has been validated and promoted by many projects due to its ability to improve on mainstream technologies such as Bitcoin and Ethereum. Off-chain technology lacks theoretical proof, and the long implementation period will bring certain time costs and security risks. In the future, the development of off-chain scaling technology will remain a mainstream approach to improving the performance of blockchain systems, strengthening fundamental measures to improve the authenticity of data on the chain, and enriching profitable businesses.

Furthermore, on-chain technologies include the processing capabilities of the main chain and the maintenance capabilities of nodes and assets, while off-chain technologies expand off-chain resources and data interaction and transmission methods. The zero-knowledge proof can link these two types of technologies with guaranteed trust and compressed computing resources. The blockchain may become a truly decentralised network when the complex off-chain data can be uploaded and used. At this stage, the key research directions are cross-chain technology, high-performance programmable technology engines and large-scale peer-to-peer networks. Specific application scenarios must be identified for deployment and implementation as reliable technical solutions.

5.2 In terms of cross-chain technical optimization

First of all, clarify the access rules between different chains. Despite the existence of many cross-chain platforms, the current cross-chain platform requirements for different links are still unclear, which is not conducive to promoting the formation of a cross-chain network or managing the security of the access chain. The examination of the security issues of the access chain is easiest to control initially. Once a failure occurs after access, it will have an incalculable impact on the whole cross-chain network.

Then, standardize cross-chain protocols and improve operability between cross-chain networks. Cross-chain protocols are the core of realizing cross-chain functions. Currently, cross-chain protocols of different cross-chain technologies are difficult to compatible with in terms of message formats and routing protocols, leading to obstacles in interoperability between different cross-chain networks. Therefore, in order to enhance the versatility and flexibility of cross-chain protocols and connect different cross-chain networks into a larger whole, it is necessary for blockchain R&D institutions and standardization organizations form a consensus in the future and jointly introduce a blockchain foundation protocol similar to TCP/IP.

At last, improve the digital identity management system to ensure the authenticity of the data on the chain. Although on-chain data cannot be tampered with and is traceable, it is more challenging to ensure the authenticity and validity of the data on-chain. On the one hand, it is necessary to establish the correspondence between on-chain and off-chain data through relevant technologies such as prophecy machines; on the other hand, it is also necessary to clarify the issue of authority and responsibility by seamlessly connecting off-chain identity with on-chain identity, thereby clarifying the issue of authority and responsibility, which is also a bridge for BT towards compliance regulation.

In general, through this review, we can not only see that blockchain technology has great potential and prospect in the future application of various industries, but also see the efficiency bottleneck restricting the real large-scale application of blockchain technology. Therefore, it is necessary to increase the research on the governance of the blockchain network, constantly standardize the operation rules of the blockchain network, and further break through the bottleneck of blockchain technology in terms of performance and efficiency, so as to finally ensure the smooth and efficient operation of the entire blockchain network, promote the large-scale application of blockchain technology, and truly exert the value of blockchain technology. The content of this paper provides a comprehensive reference for practitioners and applications related to future blockchain performance research, which has important practical significance.

Author contributions

FL has elaborated the entire content of the document and contributed ideas to the topic. The writing of the manuscript was mainly done by FL, SH, ZL, PX All of FL and JQ provided critical feedback and helped with the finalization. SH and ZL contributed to this study equally.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Ajay, K., Bharath, B., Akhil, M., Akanksh, R., and Hemavathi, P. (2018). "Intellectual property management using blockchain," in 2018 3rd International Conference on Inventive Computation Technologies, Coimbatore, India, 15-16 November 2018.

Akintade, T. (2022). understanding-the-polkadot-blockchain. Available; https://cryptotvplus.com/2022/02/understanding-the-polkadot-blockchain/.

Alharby, M., and van Moorsel, A. (2020). Blocksim: An extensible simulation tool for blockchain systems. *Front. Blockchain* 3, 28. doi:10.3389/fbloc.2020.00028

Alvi, S. T., Uddin, M. N., Islam, L., and Ahamed, S. (2022). Dvtchain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *J. King Saud Univ. - Comput. Inf. Sci.* 34, 6855–6871. doi:10.1016/j.jksuci.2022.06.014

Amen, B., Faiz, S., and Do, T.-T. (2022). Big data directed acyclic graph model for real-time Covid-19 twitter stream detection. *Pattern Recognit.* 123, 108404. doi:10.1016/j.patcog.2021.108404

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., et al. (2014). Enabling blockchain innovations with pegged sidechains. Available; http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains (Accessed 10 22, 2014).

Bai Bing, L. M., and Li, Z. (2022). Multiple rounds validation scheme to reduce rollback probability of cross-shard transactions. *Comput. Eng. Appl.* 58, 129–136. doi:10.3778/j.issn.1002-8331.2009-0080

Belchior, R., Vasconcelos, A., Guerreiro, S., and Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. *ACM Comput. Surv. (CSUR)* 54, 1–41. doi:10.1145/3471140

Bingrong, D., Shengming, J., Menglu, Z., Ming, L., Dunwei, L., and Chao, L. (2021). Evaluation model of cross-chain notary mechanism based on improved pagerank algorithm. *Comput. Eng.* 47, 26–31. doi:10.19678/j.issn.1000-3428.0056460

Brown, C., Chiu, J., and Koeppl, T. V. (2021). What drives bitcoin fees? Using segwit to assess bitcoin's long-run sustainability. *J. Financial Mark. Infrastructures* 9. doi:10.34989/swp-2022-2

Buterin, V. (2016). Chain interoperability. R3 Research Paper 9.

Buterin, V. (2015). On public and private blockchains. Available; https://blog.ethereum.org/2015/08/07/onpublic-and-private-blockchains/(Accessed 08 07, 2015).

Cai, X., Deng, Y., Zhang, L., Shi, J., Chen, Q., Zhen, W., et al. (2019). The principle and core technology of blockchain. *Chin. J. Comput.* 42, 1–15.

Cassez, F., Fuller, J., and Asgaonkar, A. (2022). Formal verification of the ethereum 2.0 beacon chain. In International Conference on Tools and Algorithms for the Construction and Analysis of Systems, Paris, Dec 22, 2022.

Castro, M., and Liskov, B., (1999). Practical byzantine fault tolerance. Available at: https://pmg.csail.mit.edu/papers/osdi99.pdf.

Chaofan, Y., Wang, L., Zhou, A., Zhang, N., Tian, H., and Xiao, J. (2021). Method and apparatus for performing multi-party secure computing based-on issuing certificate. *U. S. Pat.* 11 (038), 699.

Chen, X., Zhang, K., Liang, X., Qiu, W., Zhang, Z., and Tu, D. (2020). Hyperbsa: A high-performance consortium blockchain storage architecture for massive data. *IEEE Access* 8, 178402–178413. doi:10.1109/ACCESS.2020.3027610

Chen, Y., Li, M., Zhu, X., Fang, K., Ren, Q., Guo, T., et al. (2022). An improved algorithm for practical byzantine fault tolerance to large-scale consortium chain. *Inf. Process. Manag.* 59, 102884. doi:10.1016/j.ipm.2022.102884

Chuang, D. C., Jing, L. H., Ying, Y. X., Xiao-bing, G., Zhong-hua, L., and Bei-fang, N. (2021). Overview of blockchain technology. *Comput. Sci.* 48, 500–508. doi:10.11896/jsjkx.201200163

Collado, A., Gómez-Suárez, A., Oonishi, Y., Slawin, A. M., and Nolan, S. P. (2013). Synthesis, characterisation, and oxygen atom transfer reactions involving the first gold (i)-alkylperoxo complexes. *Chem. Commun.* 49, 10745–10747. doi:10.1039/C3CC47030J

Crain, T., Natoli, C., and Gramoli, V. (2021). "Red belly: A secure, fair and scalable open blockchain," in 2021 IEEE Symposium on Security and Privacy, USA, 24-27 May 2021.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., et al. (2016). "On scaling decentralized blockchains," in International conference on financial cryptography and data security, Barbados, February 22–26, 2016.

Dai, B., Jiang, S., Zhu, M., Lu, M., Li, D., and Li, C. (2020). "Research and implementation of cross-chain transaction model based on improved hash-locking," in International Conference on Blockchain and Trustworthy Systems, China, August 07, 2020.

Dang, H., Dinh, T. T. A., Loghin, D., Chang, E.-C., Lin, Q., and Ooi, B. C. (2019). Towards scaling blockchain systems via sharding. In Proceedings of the 2019 international conference on management of data, July 5, 2019, The Netherlands.

Decker, C., and Wattenhofer, R. (2013). Information propagation in the bitcoin network. In IEEE P2P 2013 Proceedings (IEEE), 09-11 September 2013, Trento.

Deng, X., Li, K., Wang, Z., and Liu, H. (2022). A novel consensus algorithm based on segmented dag and bp neural network for consortium blockchain. *Secur. Commun. Netw.* 2022, 1–16. doi:10.1155/2022/1060765

Ejaz, M., Kumar, T., Kovacevic, I., Ylianttila, M., and Harjula, E. (2021). Health-blockedge: Blockchain-edge framework for reliable low-latency digital healthcare applications. *Sensors* 21, 2502. doi:10.3390/s21072502

Ermilov, D., Panov, M., and Yanovich, Y. (2017). "Automatic bitcoin address clustering," in 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), Cancun, 18-21 December 2017.

Eyal, I., and Sirer, E. G. (2014). "Majority is not enough: Bitcoin mining is vulnerable," in International conference on financial cryptography and data security, Barbados, March 3-7, 2014.

Feng, L., Jia-hao, Z., Jun-jie, Z., Mu, L., De-li, K., Jie, Y., et al. (2022b). Novel hash-time-lock-contract based cross-chain token swap mechanism of blockchain. *Comput. Sci.* 49 (1), 336–344. doi:10.11896/jsjkx.210600170

Feng, L., Jie, Y., and Jia-yin, Q. (2021a). Two-party ecdsa for blockchain based on hash proof systems. *Netinfo Secur.* 19, 26. doi:10.3969/j.issn.1671-1122.2021.01.003

Feng, L., Jie, Y., Zhibin, L., and Jiayin, Q. (2021b). A secure multi-party computation protocol for universal data privacy protection based on blockchain. *J. Comput. Res. Dev.* 58, 281–290. doi:10.7544/issn1000-1239.2021.20200751

Feng, L., Yi-fan, W., Jie, Y., Ai-min, Z., and Jia-yin, Q. (2021c). Blockchain-based high-threshold signature protocol integrating dkg and bls. *Comput. Sci.* 48, 46–53. doi:10.11896/jsjkx.210200129

Frauenthaler, P., Sigwart, M., Spanring, C., and Schulte, S. (2020a). Leveraging blockchain relays for cross-chain token transfers. *Gas* 300, 600. doi:10.13140/RG.2.2.12791.37286

Frauenthaler, P., Sigwart, M., Spanring, C., and Schulte, S. (2020b). "Testimonium: A cost-efficient blockchain relay,". arXiv preprint arXiv:2002.12837.

Fröwis, M., Gottschalk, T., Haslhofer, B., Rückert, C., and Pesch, P. (2020). Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Sci. Int. Digital Investigation* 33, 200902. doi:10.1016/j.fsidi.2019.200902

Fujisaki, E., and Suzuki, K. (2007). Traceable ring signature. *Int. Workshop Public Key Cryptogr.* 4450, 181–200. doi:10.1007/978-3-540-71677-8_13

Furfaro, A., Argento, L., Saccá, D., Angiulli, F., and Fassetti, F. (2019). "An infrastructure for service accountability based on digital identity and blockchain 3.0," in IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops, France, 29 April 2019.

Gaži, P., Kiayias, A., and Zindros, D. (2019). "Proof-of-stake sidechains," in 2019 IEEE Symposium on Security and Privacy, USA, 19-23 May.

Golosova, J., and Romanovs, A. (2018). "The advantages and disadvantages of the blockchain technology," in 2018 IEEE 6th workshop on advances in information, electronic and electrical engineering, Vilnius, 08-10 November.

Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., and Gervais, A. (2020). Sok: Layer-two blockchain protocols. *Int. Conf. Financial Cryptogr. Data Secur.* 12059, 201–226.

Guo, H., and Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain Res. Appl.* 3, 100067. doi:10.1016/j.bcra.2022.100067

Han, R., Yu, J., Lin, H., Chen, S., and Esteves-Veríssimo, P. (2021). "On the security and performance of blockchain sharding,". Cryptology ePrint Archive, Paper 2021/1276.

Hepp, T., Sharinghousen, M., Ehret, P., Schoenhals, A., and Gipp, B. (2018). On-chain vs. off-chain storage for supply-and blockchain integration. *it-Information Technol.* 60, 283–291. doi:10.1515/itit-2018-0019

Herlihy, M. (2018). "Atomic cross-chain swaps," in Proceedings of the 2018 ACM symposium on principles of distributed computing, United Kingdom, July 23 - 27, 2018.

Holbrook, J. (2020). *Blockchain governance, risk, and compliance (GRC), privacy, and legal concerns*. United States: Wiley.

Huang, H., Yue, Z., Peng, X., He, L., Chen, W., Dai, H.-N., et al. (2022). Elastic resource allocation against imbalanced transaction assignments in sharding-based permissioned blockchains. *IEEE Trans. Parallel Distributed Syst.* 33, 2372–2385. doi:10.1109/TPDS.2022.3141737

Huawei, H., Wei, K., Xiaowen, P., and Zibin, Z. (2022a). Survey on blockchain sharding technology. *Comput. Eng.* 48 (1). doi:10.19678/j.issn.1000-3428.0063887

Jia, D., Xin, J., Wang, Z., and Wang, G. (2021). Optimized data storage method for sharding-based blockchain. *IEEE Access* 9, 67890–67900. doi:10.1109/ACCESS.2021.3077650

Kang, J.-S., Choi, Y.-S., Sung, M. Y., Shin, S.-H., Jeong, T. T., and Choi, Y. S. (2007). "A study of security and privacy in usn environment using hash lock approach," in International Conference On Future Information and Communication Engineering, Malaysia, Jun 26, 2015.

Karame, G. O., Androulaki, E., and Capkun, S. (2012). "Double-spending fast payments in bitcoin," in Proceedings of the 2012 ACM conference on Computer and communications security, USA, October 2012.

Khoury, D., Balian, P., and Kfoury, E. (2022). "Implementation of blockchain domain control verification (b-dcv)," in 2022 45th International Conference on Telecommunications and Signal Processing (TSP), Prague, 13-15 July 2022.

Kwon, J., and Buchman, E. (2016). Cosmos: A network of distributed ledgers. Available at; https://cosmos.network/whitepaper.

Larimer, D. (2013). Transactions as proof-of-stake. Available at; https://cryptochainuni.com/wp-content/uploads/Invictus-Innovations-Transactions-As-Proof-Of-Stake.pdf.

Lashkari, B., and Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. *IEEE Access* 9, 43620–43652. doi:10.1109/ACCESS.2021.3065880

Li, F., Li, Z.-R., and Zhao, H. (2019). Research on the progress in cross-chain technology of blockchains. *J. Softw.* 30 (6), 1649–1660. doi:10.13328/j.cnki.jos.005741

Li, Y. (2020). Overview of blockchain capacity expansion technology. *Electr. POWER ICT* 18 (6), 1–9. doi:10.16543/j.2095-641x.electric.power.ict.2020.06.001

Liang, C., Hao, D., Meng, Y., and Xin, X. (2020). Private data protection scheme for consortium blockchain based on two-layer cooperation. *J. Softw.* 31 (8), 2557–2573. doi:10.13328/j.cnki.jos.006020

Liao, K., Zhao, Z., Doupé, A., and Ahn, G.-J. (2016). "Behind closed doors: Measurement and analysis of cryptolocker ransoms in bitcoin," in 2016 APWG symposium on electronic crime research (eCrime), Toronto, 01-03 June 2016.

Liu, F., Fan, H.-Y., and Qi, J.-Y. (2022a). Blockchain technology, cryptocurrency: Entropy-based perspective. *Entropy* 24, 557. doi:10.3390/e24040557

Liu, F., Feng, Z., and Qi, J. (2022b). A blockchain-based digital asset platform with multi-party certification. *Appl. Sci.* 12, 5342. doi:10.3390/app12115342

Liu Jia-qi, Q. J.-y., and Liu, Feng (2022). Modeling and effciency analysis of blockchain public opinion deposit system based on stochastic petri net. *J. Shanghai Univ. Int. Bus. Econ.* 29, 109–124. doi:10.16060/j.cnki.issn2095-8072.2022.01.008

Liu, J. K., Wei, V. K., and Wong, D. S. (2004). "Linkable spontaneous anonymous group signature for ad hoc groups," in Australasian Conference on Information Security and Privacy, Australia, November 28-30, 2022.

Liu, Y., Zhang, L., and Zhao, Y. (2022c). Deciphering bitcoin blockchain data by cohort analysis. *Sci. Data* 9, 136–137. doi:10.1038/s41597-022-01254-0

Lombrozo, E., Lau, J., and Wuille, P. (2015). Bip141: Segregated witness (consensus layer). Available at: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki.

Lone, A. H., and Naaz, R. (2020). "Demystifying cryptography behind blockchains and a vision for post-quantum blockchains," in 2020 IEEE International Conference for Innovation in Technology (INOCON), India, 06-08 November 2020.

Mettler, M. (2016). "Blockchain technology in healthcare: The revolution starts here," in 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom), Germany, 14-16 September 2016.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Bitcoin.org.

Neudecker, T., and Hartenstein, H. (2019). "Short paper: An empirical analysis of blockchain forks in bitcoin," in International Conference on Financial Cryptography and Data Security, Nevis, February 18–22, 2019.

Nguyen, L. N., Nguyen, T. D., Dinh, T. N., and Thai, M. T. (2019). "Optchain: Optimal transactions placement for scalable blockchain sharding," in 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), USA, 07-10 July 2019.

Nofer, M., Gomber, P., Hinz, O., and Schiereck, D. (2017). *Blockchain*. Bus. Inf. Syst. Eng. 59, 183–187. doi:10.1007/s12599-017-0467-3

Nowostawski, M., and Tøn, J. (2019). Evaluating methods for the identification of off-chain transactions in the lightning network. *Appl. Sci.* 9, 2519. doi:10.3390/app9122519

Pan, C., Tang, S., Ge, Z., Liu, Z., Long, Y., Liu, Z., et al. (2019). "Gnocchi: Multiplexed payment channels for cryptocurrencies," in International Conference on Network and System Security, Japan, December 15–18, 2019.

Passerat-Palmbach, J., Farnan, T., McCoy, M., Harris, J. D., Manion, S. T., Flannery, H. L., et al. (2020). "Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data," in 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, 02-06 November 2020.

Patin, A. (2019). Technologies for private key recovery in distributed ledger systems. https://patents.google.com/patent/US10439812B2/en.

Pedersen, T. P. (1991). Non-interactive and information-theoretic secure verifiable secret sharing. In Annual international cryptology conference, August 11 - 15, 1991, Berlin.

Poon, J., and Buterin, V. (2017). Plasma:scalable autonomous smart contracts. Available at: https://www.plasma.io/plasma-deprecated.pdf.

Poon, J., and Dryja, T. (2016). "The bitcoin lightning network: Scalable off-chain instant payments,". DRAFT Version 0.5.9.2.

Prybila, C., Schulte, S., Hochreiner, C., and Weber, I. (2020). Runtime verification for business processes utilizing the bitcoin blockchain. *Future gener. Comput. Syst.* 107, 816–831. doi:10.1016/j.future.2017.08.024

Qin Wenhui, M. H., and Li, Z. (2021). Node election scheme for transaction overload processing in state sharding. *Comput. Eng. Appl.* 1, 14. doi:10.3778/j.issn.1002-8331.2109-0341

Qiu, C., Ren, X., Cao, Y., and Mai, T. (2020). Deep reinforcement learning empowered adaptivity for future blockchain networks. *IEEE Open J. Comput. Soc.* 2, 99–105. doi:10.1109/OJCS.2020.3010987

Qiwu, Z. (2020). *Research on blockchain scalability based on State Channel And cross-chain protocol*. Shanghai: Master's thesis, Shanghai Jiao Tong University.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21, 120–126. doi:10.1145/359340.359342

Ruan, P., Chen, G., Dinh, T. T. A., Lin, Q., Ooi, B. C., and Zhang, M. (2019). Fine-grained, secure and efficient data provenance on blockchain systems. *Proc. VLDB Endow.* 12, 975–988. doi:10.14778/3329772.3329775

Schwartz, D., Youngs, N., and Britto, A. (2014). The ripple protocol consensus algorithm. *Ripple Labs Inc. White Pap.* 5, 151.

Shahsavari, Y., Zhang, K., and Talhi, C. (2019). "Performance modeling and analysis of the bitcoin inventory protocol," in 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), USA, 04-09 April 2019.

Shahsavari, Y., Zhang, K., and Talhi, C. (2022). Toward quantifying decentralization of blockchain networks with relay nodes. *Front. Blockchain* 5, 812957. doi:10.3389/fbloc.2022.812957

Sigwart, M., Borkowski, M., Peise, M., Schulte, S., and Tai, S. (2019). "Blockchain-based data provenance for the internet of things," in Proceedings of the 9th International Conference on the Internet of Things, Italy, Nov 29, 2022.

Sompolinsky, Y., and Zohar, A. (2015). "Secure high-rate transaction processing in bitcoin," in International conference on financial cryptography and data security, Puerto Rico, January 26-30, 2015.

Sonnino, A., Bano, S., Al-Bassam, M., and Danezis, G. (2020). "Replay attacks and defenses against cross-shard consensus in sharded distributed ledgers," in 2020 IEEE European Symposium on Security and Privacy (EuroS&P), Italy, 07-11 September 2020.

Stark, J. (2018). Making sense of ethereum's layer 2 scaling solutions: State channels, plasma, and truebit. Available at: https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4 (Accessed 02 12, 2018).

Tam Vo, H., Wang, Z., Karunamoorthy, D., Wagner, J., Abebe, E., and Mohania, M. (2018). "Internet of blockchains: Techniques and challenges ahead," in 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), Canada, 30 July 2018.

Tao, L., Lu, Y., Ding, X., Fan, Y., and Kim, J. Y. (2022). Throughput-oriented associated transaction assignment in sharding blockchains for iot social data storage. *Digital Commun. Netw.* 8, 885–899. doi:10.1016/j.dcan.2022.05.024

Teutsch, J., and Reitwießner, C. (2019). "A scalable verification solution for blockchains,". arXiv preprint arXiv:1908.04756.

Thomas, S., and Schwartz, E. (2015). A protocol for interledger payments. Available at: https://interledger.org/interledger.pdf.

Tian, F. (2016). "An agri-food supply chain traceability system for China based on rfid and blockchain technology," in 2016 13th international conference on service systems and service management (ICSSSM), Kunming, 24-26 June 2016.

Uddin, M. A., Stranieri, A., Gondal, I., and Balasubramanian, V. (2021). A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain Res. Appl.* 2, 100006. doi:10.1016/j.bcra.2021.100006

Van Saberhagen, N. (2013). Cryptonote v 2.0. Available at: https://cryptonote.org/whitepaper.pdf (Accessed 10 17, 2013).

Wang, C., and Chu, X. (2020). "Performance characterization and bottleneck analysis of hyperledger fabric," in 2020 IEEE 40th International Conference on Distributed Computing Systems, Singapore, Dec. 1 2020.

Wang, G., Shi, Z. J., Nixon, M., and Han, S. (2019a). "Sok: Sharding on blockchain," in Proceedings of the 1st ACM Conference on Advances in Financial Technologies, China, October 2019.

Wang, J., Chenchen, H., Xiaofeng, Y., Yongjun, R., and Sherratt, S. (2022a). Distributed secure storage scheme based on sharding blockchain. *Comput. Mater. Continua* 70, 4485–4502. doi:10.32604/cmc.2022.020648

Wang, J. (2022). Scale out blockchain with asynchronized consensus zones. *U. S. Pat.* 11 (228), 439.

Wang, J., and Wang, H. (2019). "Monoxide: Scale out blockchains with asynchronous consensus zones," in 16th USENIX symposium on networked systems design and implementation, Boston, February 26–28, 2019.

Wang, S., Li, H., Chen, J., Wang, J., and Deng, Y. (2022b). Dag blockchain-based lightweight authentication and authorization scheme for iot devices. *J. Inf. Secur. Appl.* 66, 103134. doi:10.1016/j.jisa.2022.103134

Wang, T., Ma, W., and Luo, W. (2019b). Information sharing and secure multi-party computing model based on blockchain. *Comput. Sci.* 46, 162–168. doi:10.11896/j.issn.1002-137X.2019.09.023

Wątorek, M., Drożdż, S., Kwapień, J., Minati, L., Oświęcimka, P., and Stanuszek, M. (2021). Multiscale characteristics of the emerging global cryptocurrency market. *Phys. Rep.* 901, 1–82. doi:10.1016/j.physrep.2020.10.005

Wen, J. (2022). Performance optimization of blockchain sharding system combined with deep reinforcement learning. *Comput. Eng. Appl.*, 1–9. doi:10.3778/j.issn.1002-8331.2203-0142

Wenlin, L. (2020). *Ethereum throughput bottleneck analysis and optimization research. Master's thesis*. China: Xiangtan University.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. yellow Pap.* 151, 1–32.

Xiaoqiong, X., Gang, S., and Long, L. (2022). Sharding algorithm based on evolutionary game in the iot-blockchain. *J. Univ. Electron. Sci. Technol. China* 51 (3), 363–370. doi:10.12178/1001-0548.2022029

Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., and Liu, Y. (2019). A survey on the scalability of blockchain systems. *IEEE Netw.* 33, 166–173. doi:10.1109/MNET.001.1800290

Xu, J., Ackerer, D., and Dubovitskaya, A. (2021a). "A game-theoretic analysis of cross-chain atomic swaps with htlcs," in 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), USA, 07-10 July 2021.

Xu, X., Sun, G., Luo, L., Cao, H., Yu, H., and Vasilakos, A. V. (2021b). Latency performance modeling and analysis for hyperledger fabric blockchain network. *Inf. Process. Manag.* 58, 102436. doi:10.1016/j.ipm.2020.102436

Xu, X., Sun, G., and Yu, H. (2021c). "An efficient blockchain pbft consensus protocol in energy constrained iot applications," in 2021 International Conference on UK-China Emerging Technologies, China, 04-06 November 2021.

Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2019). "Blockchain technology overview,". arXiv preprint arXiv:1906.11078.

Yao, Y., Kshirsagar, M., Vaidya, G., Ducrée, J., and Ryan, C. (2021). Convergence of blockchain, autonomous agents, and knowledge graph to share electronic health records. *Front. Blockchain* 4, 661238. doi:10.3389/fbloc.2021.661238

Yu Hui, L. J., and Zhang, Z. (2017). Research on scaling technology of bitcoin blockchain. *J. Comput. Res. Dev.* 54, 2390–2403. doi:10.7544/issn1000-1239.2017.20170416

Yuan Yong, W. F.-Y. (2016). Blockchain: The state of the art and future trends. *ACTA AUTOM. SIN.* 42, 481–494. doi:10.16383/j.aas.2016.c160158

Zeng, S., Yuan, Y., Xiao-Chun, N. I., and Fei-Yue, W. (2019). Scaling blockchain towards bitcoin: Key technologies, constraints and related issues. *Acta Autom. Sin.* 45 (6), 1015–1030. doi:10.16383/j.aas.c180100

Zhang, J., Hong, Z., Qiu, X., Zhan, Y., Guo, S., and Chen, W. (2020). "Skychain: A deep reinforcement learning-empowered dynamic blockchain sharding system," in 49th International Conference on Parallel Processing-ICPP, Edmonton, 17 - 20 Aug 2020.

Zhao, G., Shuaiyin, G., Shengli, Z., Lingyang, S., and Hui, W. (2020). Analysis of cross-chain technology of blockchain. *J. Internet Things* 4, 36–49. doi:10.11959/j.issn.2096?3750.2020.00162

Zhuoyan, X., and Xuan, Z. (2021). Survey on crosschain technology. *Appl. Res. Comput.* 38, 341–346. doi:10.19734/j.issn.1001-3695.2020.01.0025