Journal of Intelligent Management Decision
https://www.acadlore.com/journals/JIMD

High-Performance Carbon Cycle Supply Data Sharing Method Based on Blockchain Multichain Technology

Yuanjun Liu[1], Lin Zhang[2*], Ashim Khadka[3]

[1] Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, 223003 Huaian, China
[2] Faculty of Management Engineering, Huaiyin Institute of Technology, 223003 Huaian, China
[3] Nepal College of Information Technology, Pokhara University, 44700 Lalitpur, Nepal

* Correspondence: Zhang lin (zlmjl@hyit.edu.cn)

Received: 02-05-2024 **Revised:** 03-16-2024 **Accepted:** 03-26-2024

Citation: Y. J. Liu, L. Zhang, and A. Khadka, "High-performance carbon cycle supply data sharing method based on blockchain multichain technology," *J. Intell Manag. Decis.*, vol. 3, no. 2, pp. 77–90, 2024. https://doi.org/10.56578/jimd030202.

Abstract: In the evolution of blockchain technology, the traditional single-chain structure has faced significant challenges, including low throughput, high latency, and limited scalability. This paper focuses on leveraging multichain sharding technology to overcome these constraints and introduces a high-performance carbon cycle supply data sharing method based on a blockchain multichain framework. The aim is to address the difficulties encountered in traditional carbon data processing. The proposed method involves partitioning a consortium chain into multiple subchains and constructing a unique "child/parent" chain architecture, enabling cross-chain data access and significantly increasing throughput. Furthermore, the scheme enhances the security and processing capacity of subchains by dynamically increasing the number of validator broadcasting nodes and implementing parallel node operations within subchains. This approach effectively solves the problems of low throughput in single-chain blockchain networks and the challenges of cross-chain data sharing, realizing more efficient and scalable blockchain applications.

Keywords: Blockchain; Parallel processing; Cross-chain access; Sharding technology

1 Introduction

Blockchain technology [1], as a decentralized distributed ledger technology, offers effective technical support to address the multiple challenges currently faced by the carbon market, including issues such as ensuring data authenticity, weak regulation, and information asymmetry, through its unique characteristics like decentralization, traceability, immutability, anti-counterfeiting, multi-party consensus mechanism, and transparency of rules. The application of blockchain technology can not only significantly enhance the credibility of carbon market data but also strengthen the regulation of carbon trading, increase market transparency, enhance the traceability of carbon emission rights, and ensure the security of transactions. However, current blockchain systems like Bitcoin and Ethereum have a maximum transaction throughput of only 7 TPS and less than a hundred, respectively, which significantly limits their potential application in the carbon market, as these throughputs are far from meeting the needs of Internet-level applications. To overcome this limitation, it is urgently necessary to further research and develop higher-performance blockchain technologies to improve processing capacity, reduce transaction confirmation time, and thus meet the needs of large-scale applications in the carbon market.

This paper focuses on the issue of optimizing blockchain performance, aiming to enhance the operational efficiency of the blockchain system by constructing a parallel multichain blockchain model. Based on this, the paper discusses the security of the parallel multichain blockchain model and the issues of cross-chain transactions from the perspectives of network sharding and transaction sharding. The main work of this study includes the following aspects:

(1) By designing an interactive "child-parent chain" structure to realize cross-chain access, this study provides an effective solution for improving carbon data sharing and processing efficiency between different blockchains. This structure helps to break down the information silos existing in traditional blockchain systems, thereby promoting the circulation and interoperability of data.

(2) To optimize blockchain performance, this study constructs a parallel multichain blockchain model from the perspective of system architecture. The core of this model is to change the traditional single-layer chain structure of

blockchains, innovatively processing transactions through the adoption of sharding technology.

(3) The node sharding strategy proposed in this study, by finely dividing and optimizing node functions, successfully achieves an increase in throughput while ensuring the security within subchains. The essence of this strategy is to distribute the blockchain's block-producing and validation broadcasting operations to different nodes, and to enhance the performance and security of the entire network by dynamically increasing the number of validation broadcasting nodes.

By adopting an interactive multichain structure and sharding technology, this study effectively improves the processing capacity and throughput of the blockchain, while fully utilizing distributed computing and storage resources. This design is of significant importance for accelerating carbon data verification and transaction speed, and for enhancing the efficiency and credibility of carbon trading.

2 Literature Review and Problems

2.1 Sharding Technology and Multichain Structures

To improve the transaction throughput of blockchain, a common method is to adjust key parameters of the blockchain system, such as reducing the block generation interval time or increasing the block size [2]. The basic principle of this method is to process more transactions within the same timeframe, thereby enhancing the overall throughput of the system. However, the effectiveness of this approach in improving blockchain performance has certain limitations. For example, even if the Bitcoin network's block size is expanded to 8MB, its system throughput is unlikely to exceed 100 transactions per second (TPS). Moreover, increasing the block size may lead to network congestion, and accelerating block generation rate might increase the risk of system forks, thus this method cannot fundamentally solve the problem of inadequate blockchain performance.

Current research on blockchain performance optimization mainly focuses on several key technological areas: sharding technology, parallel multichain architectures, off-chain state channel technology, and cross-chain technology. Sharding technology, originally used to solve the performance bottleneck of large-scale databases, reduces the storage burden on individual nodes by horizontally or vertically dividing data, thereby improving system performance. The systematic application of sharding technology in the blockchain field began in 2016, when Luu et al. [3] and others proposed Elastico-a secure sharding protocol for permissionless blockchains. Subsequently, Dang et al. [4] improved the Byzantine Fault Tolerance (BFT) consensus protocol to enhance transaction processing capability in a sharded environment. In 2018, Zamani et al. [5] introduced the Rapid Chain blockchain framework based on sharding technology, which significantly reduced the storage cost of blockchain scalability using state sharding technology and achieved nearly linear growth in transaction throughput. That same year, Ethereum launched its Ethereum 2.0 sharding scheme, which enhanced the system's overall efficiency by processing transactions on shard chains in parallel and aggregating the results on the main chain [6]. As of December 31, 2021, Ethereum further optimized its ETH2.0 sharding scheme, improving the design of shard proposers. In this new model, the beacon chain integrated a block proposer mechanism, and transactions were processed through execution payloads with shard data, simplifying the original design [7].

The core idea of multichain architectures is similar to sharding technology, with the basic principle being to store different transaction data on multiple independent chains for parallel processing. As the number of chains increases, the system performance shows near-linear growth. In this field, in 2016, Kwon and Buchman [8] proposed Cosmos, a heterogeneous network system. Cosmos consists of two parts: Hub as the network's hub, and Zones as independent blockchains that process specific transactions or applications. Cosmos solve the interaction problems between different blockchains through relay technology and the Tendermint consensus algorithm, achieving inter-chain connectivity and asset exchange. Meanwhile, scholar Huiyong Zhang, while serving as the head of R&D for ThunderChain, proposed a homogenous multichain architecture, in which each chain has the same structure and status, enabling ThunderChain to achieve high transaction throughput capable of handling Internet-level data [9]. Additionally, in 2018, the Telegram team initiated the Telegram TON project, a blockchain platform with a multichain architecture that supports various on-chain application services. The notable feature of the TON project is its strong scalability, capable of adapting to diverse application demands.

2.2 Off-Chain Channels and Cross-Chain Technology

Off-chain state channel technology is an effective method to increase the transaction throughput of blockchain systems. It relieves the burden on the main chain by processing transactions outside the main blockchain, thereby enhancing transaction speed and efficiency. This technology encompasses solutions such as sidechains and the Lightning Network. In 2014, Adam Back and his colleagues proposed the sidechain technology, allowing Bitcoin or other cryptocurrencies to be transacted on another blockchain, thus increasing the transaction throughput of the Bitcoin network. In January 2016, Poon and Dryja [10] launched the Lightning Network, which supports small and fast transactions through off-chain payment channels, significantly reducing the main blockchain's burden of processing a large number of transactions. Based on the Lightning Network, in 2017, Miller and others proposed

the Sprites scheme, which optimized the transaction settlement mechanism, shortened the processing time for large transactions, and reduced the complexity of channel collateral. These innovations provide a more efficient way of processing transactions for blockchain systems, especially in effectively relieving the pressure on the main chain when handling a large number of small transactions [11].

In 2013, Spilman and his team proposed a unidirectional channel payment protocol based on the Bitcoin system, allowing the payer to transfer funds to the payee an unlimited number of times through a dedicated channel. The limitation of this unidirectional channel is that it cannot support the reversal of funds from the payee to the payer. To overcome this limitation, in 2015, Decker and Wattenhofer introduced the Duplex micropayment channels scheme, introducing the concept of bidirectional payment channels. This allows users to make fast bidirectional payments off-chain without waiting for on-chain confirmation, thus providing a more instant payment experience. Expanding on this concept further, in 2019, Pan et al. [12] proposed the multi-directional payment channel scheme Gnocchi, under this scheme, participants establish constraints and trust by locking deposits in smart contracts, the scheme supports bidirectional payments and multi-user interactions, increasing the flexibility and efficiency of off-chain payment channels.

The development of cross-chain technology effectively solves the problem of value silos in the blockchain ecosystem, achieving interoperability between different blockchains, and making value exchange and transfer possible. In 2019, Borkowski et al. [13], addressing the fragmentation problem in blockchain technology research and development, created a cross-blockchain interoperability platform. This platform promotes collaborative work between chains in a multi-chain coexistence environment, enhancing the functionality and efficiency of the entire blockchain ecosystem. That same year, Chen and Wang [14] proposed the SSChain scheme based on Bitcoin. By converting cross-shard transactions into intra-shard transactions, it significantly reduced communication costs and introduced a market incentive mechanism to improve system security and stability. In 2016, Wood [15] released the Polkadot whitepaper, proposing a heterogeneous cross-chain technology architecture that includes relay chains and parachains. The former is responsible for cross-chain data interaction and consensus security, while the latter focuses on meeting diverse application needs. In 2018, the Fusion blockchain project introduced distributed key control technology, achieving decentralized cross-chain interaction [16]. This technology, through innovative key management and encryption methods, makes information and asset exchange between different blockchains more secure and efficient.

2.3 Research Challenges

Despite blockchain technology being applied in various fields and achieving initial success, research both domestically and internationally still faces key challenges in optimizing blockchain performance:

(1) Sharding Technology: The Elastico protocol proposed by Luu et al. [3], the Rapid Chain framework developed by Zamani et al. [5], and the Ethereum 2.0 sharding solution by Ethereum have made significant progress in enhancing blockchain processing capability and efficiency. However, the implementation of these technologies introduces new security challenges. Specifically, the sharding mechanism might reduce the overall network security, as attackers controlling a sufficient number of nodes in a shard could potentially manipulate or alter the transaction records of that shard, threatening the integrity of the entire blockchain network. Moreover, the reduction in the number of nodes per shard due to sharding technology might further decrease the security of individual shards [17].

Current research on network sharding typically involves dividing nodes through random assignment. While simple, this method does not fully consider the behavioral characteristics of nodes, potentially leading to the congregation of malicious nodes in specific shards. This congregation not only increases the risk of Sybil attacks but may also reduce the working efficiency of shards. Therefore, despite the significant potential of sharding technology in enhancing transaction throughput, its security issues require further research and resolution to ensure the stability and safety of the blockchain network.

(2) Multichain Architecture: The Cosmos developed by Kwon and Buchman [8] and the TON project launched by the Telegram team are designed to improve the overall system throughput and scalability through multiple parallel blockchains. However, in such an architecture, each independently operating chain must maintain its security, posing certain challenges. Since resources might be dispersed across multiple chains, this could make individual chains, especially those relatively smaller or with fewer validator nodes, more susceptible to security attacks. This situation demands additional security mechanisms and strategies to ensure the stability and safety of each chain, particularly in the face of potential malicious attacks.

(3) Off-Chain State Channel Technology: The sidechain technology proposed by Adam Back, the Lightning Network developed by Poon and Dryja [10], and the Sprites scheme proposed by Miller et al. [11] aim to relieve the main chain's burden by processing transactions outside the main blockchain. These technologies allow for faster and more flexible transactions while maintaining the core advantages of blockchain. However, the security of off-chain channels greatly depends on accurate transaction records and effective dispute resolution mechanisms. If these channels are flawed in design or implementation, it could lead to the theft of funds or alteration of transaction records.

(4) Cross-Chain Technology: The cross-chain interoperability platform developed by Borkowski et al. [13]'s team and the Polkadot project founded by Wood [15] focus on achieving interoperability between different blockchains, thus facilitating broader network collaboration and asset flow. This technology allows different blockchain systems to share information and execute transactions, bringing unprecedented flexibility and scalability to the blockchain ecosystem. However, the security of cross-chain interactions is based on the security of the participating chains. This means that if any chain in the network is attacked or compromised, it could negatively affect the security and stability of the entire cross-chain network [18].

This study adopts an innovative approach in implementing consortium chain sharding, dividing the consortium chain into multiple subchains and considering dynamic node configuration. Specifically, nodes in subchains are further categorized into block-producing nodes and validator broadcasting nodes. To enhance the security and effectiveness of the validation process, we merge the validator broadcasting nodes of mutually transacting subchains to jointly execute validation broadcasting operations. This strategy of dynamically increasing the number of nodes helps enhance overall security, as more nodes participate in the validation process, reducing the risk of single or few nodes being attacked.

In the multichain structure, when the most vulnerable subchain is attacked, due to the interdependent relationships between subchains, if one chain's interests are harmed, other subchains will refuse to transact with it. This mechanism is akin to an "AND" gate operation, where transactions can only proceed smoothly when all subchains are unharmed, thus ensuring the success of the entire transaction. If any subchain is attacked and its interests are compromised, the transaction will be terminated, and the compromised chain will be isolated. This design not only safeguards the stability of the multichain structure but also enhances the security of cross-chain technology, effectively preventing the spread of security vulnerabilities throughout the network.

3 Framework Model

3.1 Carbon Trading Process Framework

This study demonstrates the entire process of data interaction and carbon flow by simulating the carbon trading process involving five key entities: manufacturers, logistics providers, collection centers, carbon processing plants, and recycling centers. The specific simulation process is as follows:

(1) Manufacturer Carbon Emission Records: Manufacturers generate carbon emissions during the production process and record the emission data.

(2) Carbon Emissions from Logistics Providers: Logistics providers are responsible for transporting products from manufacturers to sales centers and record related carbon emission data.

(3) Classification and Processing at Collection Centers: Collection centers classify and process recycled old products, recording the carbon reduction data generated by the processing.

(4) Processing and Emission Reduction at Carbon Processing Plants: Carbon processing plants receive the classified products from the collection centers, process them to reduce carbon emissions.

(5) Closed-loop Utilization at Recycling Centers: Recycling centers acquire the processed carbon materials, achieving resource closed-loop utilization.

As shown in Figure 1, throughout the process, the carbon emissions and reduction data generated by each participant are recorded and tracked using blockchain technology. Based on these data, the parties engage in carbon trading, simulating the flow of carbon throughout the entire lifecycle of the industry chain, which aids in developing effective carbon data management schemes.

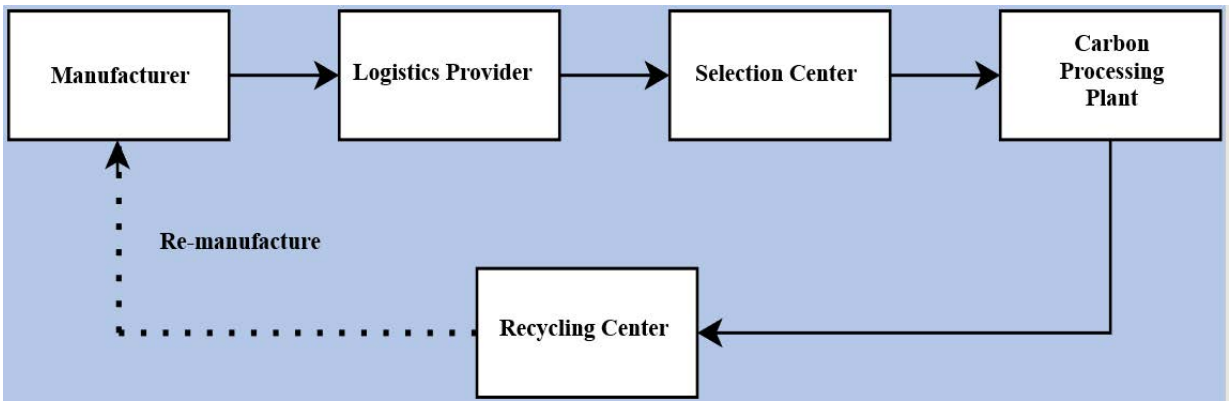

Figure 1. Flowchart of carbon trade

3.2 Cross-Chain Access Architecture

This paper presents an innovative "child/parent" chain architecture for partitioning a consortium chain into multiple private chains and facilitating efficient and secure cross-chain interactions through a relay chain. Here is a basic design scheme:

(1) Network Architecture:

Private Chain (Child Chains): Internal data and transactions of carbon enterprises are run and managed by dedicated block-producing nodes, which not only ensure the efficiency and accuracy of data processing but also implement strict access control measures and maintain high data privacy.

Consortium Chain (Parent Chain): Data originates from the relay chain and is collectively managed and monitored by several participating carbon enterprises.

Relay Chain: Each pair of transacting carbon enterprises is connected through a common relay chain, which serves as a bridge between the consortium chain and their respective private chains. It is responsible for verifying and storing cross-chain data while also ensuring the smooth supply of data from the private chains to the consortium chain (parent chain).

(2) Node Cross-Chain Access Mechanism:

Node Registration and Authentication: Validator broadcasting nodes on private chains must complete registration and authentication processes on the relay chain to obtain permission for cross-chain access. This process covers several key steps: identity verification to ensure the authenticity and reliability of each node's identity; permission allocation based on the node's role and responsibilities; and the generation of security credentials, providing each authenticated node with a unique security identifier to verify its identity and permissions during cross-chain interactions.

Node Role Definition: The paper defines the roles and responsibilities of various private chain nodes to optimize the cross-chain interaction process. For example, with two transacting subchains, the validator node of the previous subchain is responsible for providing the necessary data, while nodes of the latter subchain focus on data reception and preliminary processing. Once these two groups of nodes merge on the relay chain, they jointly handle data validation and broadcasting operations.

(3) Data Interaction and Verification Process:

Data Request: In this architecture, validator broadcasting nodes on private chains are empowered to initiate data requests to other private chain nodes through the relay chain. Through the relay chain, these validator broadcasting nodes can effectively request, receive, and verify data from other private chains.

Cross-Chain Verification: Smart contracts on the relay chain are responsible for coordinating and verifying requests and feedback from private chain nodes, ensuring the legality and security of the data.

Result Feedback: Transactions or data request results verified and confirmed by smart contracts on the relay chain are promptly and accurately fed back to the requester through the relay chain.

(4) Operation Process:

Initiating Cross-Chain Transactions: After completing the block production phase, private chains need to engage in cross-chain interactions, initiating cross-chain transaction requests to the relay chain.

Data Encryption and Packaging: Once a cross-chain transaction request is triggered, related data is first encrypted to ensure security and privacy during transmission [19]. This encrypted data is packaged into a format compatible with the system standards for compatibility and recognition across different chains. After these steps, validator broadcasting nodes on the subchain are responsible for sending this encrypted and formatted data packet to the relay chain.

Relay Chain Verification: Smart contracts deployed on the relay chain [20] first receive data from the previous subchain. After receiving the data, the smart contract [21] further notifies the next subchain to initiate the verification operation. Once the next subchain receives the notification, it first performs identity verification to confirm the legality and security of the interaction. After completing identity verification, the validator broadcasting nodes of this subchain merge with those of the previous subchain, forming a joint validation group to verify the legality and integrity of the data.

Confirmation and Synchronization: Once the cross-chain data verification process on the relay chain is successfully completed and confirmed to be error-free, the corresponding transaction results are recorded on the relay chain. This recording step includes not only the detailed contents of the transaction but also information related to the verification process, ensuring the transparency and traceability of the entire transaction. After these records, smart contracts on the relay chain are responsible for feeding back the verified transaction results to the related subchains.

Data Merging: After the entire cross-chain transaction process is successfully completed, smart contracts on the relay chain use a logic mechanism similar to an "AND" gate to process data. This means that only when all relevant subchain transactions are successfully verified and confirmed, the relay chain triggers the final data merging and packaging process. Subsequently, the smart contracts of the consortium chain summarize and package these verified data into a unified and standardized dataset. This dataset contains transaction information from all relevant subchains, maintaining data integrity and coherence. Finally, the packaged data is sent to the consortium chain.

(5) Security and Privacy Measures:

Access Control: Only authorized validator nodes can access and participate in cross-chain transactions.

Identity Verification and Authorization: Strict identity verification and authorization processes are implemented for parties involved in cross-chain transactions to ensure the security and compliance of the transactions. Specifically, when a subchain initiates a cross-chain transaction request, the request first undergoes identity verification on the relay chain to ensure the legitimacy and security of the request source. Subsequently, when the request is passed to the next subchain, that subchain also performs the necessary identity verification steps. This process includes verifying the identity information of the requester and checking their permissions. Only after passing these verifications, will the validator broadcasting nodes of the next subchain participate in the transaction, performing data processing or providing the necessary response.

3.3 "Child/Parent" Chain Structure Model

Currently, most blockchain systems still adopt a single-chain structure. However, with the rapid development of blockchain technology and the increasingly diverse application scenarios, the single-chain structure faces challenges in processing a large volume of transaction data and supporting complex application requirements. To meet the growing needs for digital asset diversity and enhance the overall performance of blockchain systems, this paper proposes a parallel multichain blockchain model that changes the traditional single-chain structure [22].

The core of this model is the use of sharding technology to divide the original main chain into multiple relay chains and further subdivide into more subchains at a 2n ratio to increase the number of subchains. The distribution of nodes on each subchain is optimized according to data characteristics and transaction requirements to ensure efficiency and security.

To further optimize blockchain performance, this model divides nodes within private chains based on their behavioral characteristics and data features. In each private chain, nodes are further divided into block-producing nodes and validator broadcasting nodes. Block-producing nodes are responsible for independently executing block production, while validator broadcasting nodes require assistance from the next private chain for validation, thus ensuring the validity and security of transactions. This layered node role assignment and multichain parallel working mode provide a coordinated operating framework for the entire system.

Each subchain operates independently but collaboratively supports complex application scenarios. In the carbon trading process, when manufacturers transact with logistics providers, the manufacturer's block-producing nodes are responsible for block generation. During the validation and broadcasting phase, to enhance the security and reliability of the transaction, the validator broadcasting nodes of the manufacturer and logistics provider are merged and execute validation on the L1 relay chain. Once verified on the L1 chain, the relevant data is recorded in the L1 chain. At this point, the validator broadcasting nodes of the manufacturer and logistics provider share and save the relevant carbon trading data.

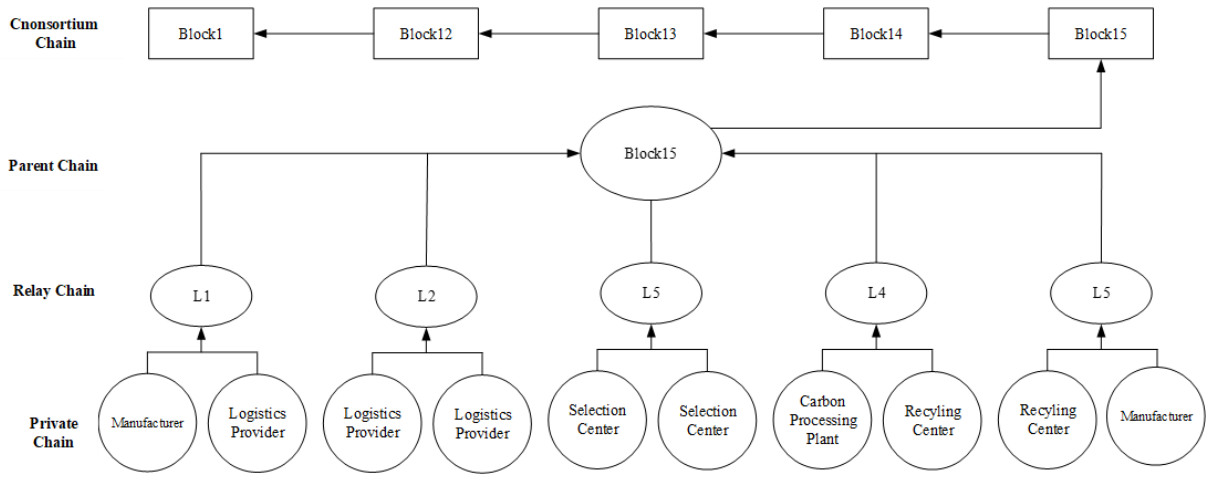

Figure 2. Parallel multichain blockchain model

As the transaction progresses, this process continues sequentially on L2, L3, L4, L5, and other relay chains, ensuring data integrity and security at each stage. This method is similar to an "AND" gate operation, ensuring that only transaction data verified by all relay chains can be uploaded to the consortium chain. Ultimately, the transaction forms a complete record of carbon cycle data sharing on the consortium chain. This mechanism not only safeguards the integrity and accuracy of carbon trading data but also provides an efficient and secure data sharing and verification method for the entire carbon trading ecosystem. The structure and working mechanism of the parallel multichain

blockchain model are illustrated in Figure 2, demonstrating how to enhance the system's processing capacity and throughput while ensuring data integrity and security.

The parallel multichain blockchain model proposed in this paper aims to realize the partitioned processing of blockchain data, supporting concurrent operations of complete blockchains formed by multiple replicas within a chain while ensuring that each subchain maintains a high degree of autonomy and the overall system preserves the consistency of the global blockchain. In this model, each chain is independently responsible for its block production, while inter-chain transactions are coordinated through concurrent operations, achieving global consistency and efficiency.

3.4 Performance Analysis of the "Child/Parent" Chain Structure Transaction Throughput Model

Increasing block size and Gas limit can enhance the system's transaction processing capacity, but often at the expense of decentralization. The parallel multichain blockchain model proposed in this paper utilizes sharding technology to divide the consortium chain into multiple subchains, thereby improving the system's overall throughput through these parallel-running subchains. To study the impact of this model on the blockchain system's throughput, we designed the following experiment:

Assuming that the traditional single-chain architecture has a throughput of 10 TPS, and in the parallel multichain blockchain model, we set different degrees of subchain granularity, namely 5, 10, 20, and 30. In this model, the consensus time for each subchain fluctuates by ±10% compared to the consensus time of the single-chain architecture. The experiment aims to compare the relationship between the throughput of the single-chain and multichain models under different degrees of subchain granularity.

Table 1. Throughput comparison by subchain granularity

Shard Granularity	Multi-Chain TPS	TPS Improvement Factor
5.0	50.38	5.03
10.0	99.78	9.98
20.0	198.32	19.83
30.0	297.13	29.71

Data analysis from Table 1 shows that under the condition of ±10% fluctuation in subchain consensus time, the transaction throughput of the parallel multichain blockchain shows a linear growth trend with the increase in subchain granularity. In this study, one carbon cycle supply chain data consists of 5 transactions, hence dividing the parent chain into 5 relay chains, each further divided into 10 subchains. Under this structure, data is formed between every two subchains through transaction consensus, with the set subchain granularity being 10. The results show that the throughput of this parallel multichain structure is significantly higher than that of the traditional single-chain architecture [23].

In terms of storage capacity, the traditional single-chain model requires all nodes to store complete and identical data, leading to a considerable storage burden. In contrast, in the parallel multichain structure proposed in this paper, each subchain only needs to save a portion of the data. After two subchains complete a transaction, the relevant data portion is uploaded to the relay chain. After the entire cycle process is completed, some data is uploaded to the consortium chain. This layered and stepwise data storage approach not only enhances the efficiency of data management but also significantly reduces the overall storage demand, making the system more efficient and scalable.

4 Dynamic Nodes

In traditional single-chain blockchain networks, all nodes are concentrated on the same chain, providing the network with strong node computing power. In such a scenario, to initiate a malicious attack and alter data on the chain, an attacker would need to control more than 51% of the network's node computing power, which is nearly impossible in a vast network, making the risk of conspiratorial attacks very low [24].

However, when adopting sharding technology and splitting the blockchain network into multiple independently operating subchains, nodes are dispersed across these subchains, with each subchain having relatively fewer nodes. As the granularity of splitting increases, the number of nodes in each subchain decreases, meaning a reduction in distributed verification and consensus participants, which could lead to decreased network security since a smaller number of nodes might be more susceptible to attacks and manipulation.

To address this issue, this paper proposes a cross-chain mechanism and enhances network security by dynamically increasing the number of nodes. In this design, when subchain A transacts with subchain B, A is responsible for completing the block production phase, while B needs to validate A's block, forming a joint validation logic. This mechanism prevents individual subchains from independently validating their own blocks, ensuring the authenticity and security of transactions. The correct transaction logic is that after A completes the block production phase, A and

B jointly validate the block to ensure the transaction's legitimacy and security. A schematic of this design, as shown in Figure 3, demonstrates the working principle and process of the cross-chain validation mechanism.

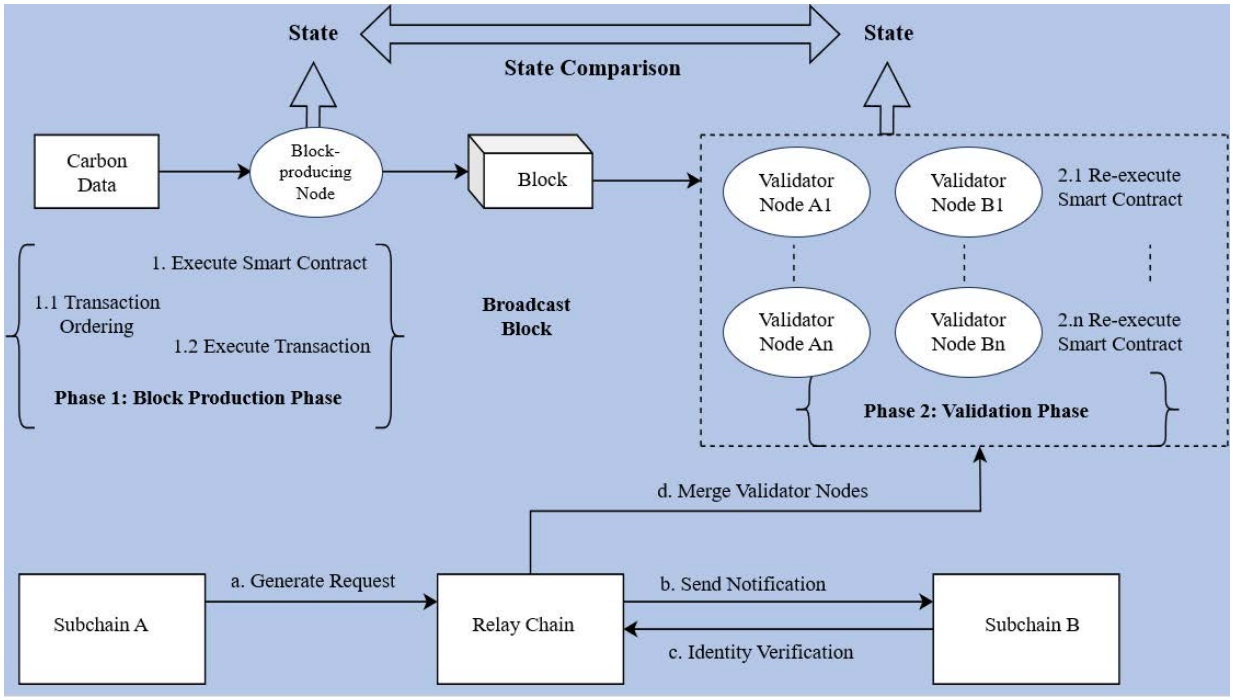

Figure 3. Diagram of dynamic nodes

In the parallel multichain blockchain model proposed in this paper, when subchain A completes the block production phase and generates state A1, it initiates a collaborative validation request to the relay chain. Upon receiving this request, subchain B first verifies the identity of the initiating subchain A and confirms the target chain. Subsequently, the relay chain integrates the validator nodes of subchain A and B into a common validation group for the upcoming verification process.

Entering the block broadcasting phase, this common validation group validates subchain A's new block based on the distributed consensus mechanism, generating state B2. The system then compares state A1 with B2 to determine the legality and validity of the new block. If the verification result is valid, the nodes responsible for validation (also broadcasting nodes) will broadcast this record on the relay chain, allowing other chain nodes to access and confirm.

Finally, subchain B accesses the relevant data on the relay chain through a cross-chain access mechanism for subsequent operations. This collaborative validation mechanism effectively avoids the unreliability of subchain A's solitary self-validation and enhances the entire blockchain network's security, attack resistance, decentralization level, fault tolerance, and reliability by increasing the number of validator nodes. Moreover, this mechanism also enhances the fairness of the consensus process. In this mechanism, subchain B acts as an auxiliary validator, providing reliable and authoritative verification results for the data produced by subchain A. This not only offers additional trust and authority to subchain A's carbon trading data but also contributes to the robustness and reliability of the entire system.

4.1 Single-Chain Node Sharding Analysis and Comparison

Unlike existing blockchain systems such as Omniledger or Monoxide, which typically use a random selection method to divide subchains, the model proposed in this paper divides subchain nodes based on business units, and transactions between subchains have close connections. When one subchain colludes with a subsequent subchain to launch an attack, such behavior directly impacts the interests of the subsequent subchain, thereby reducing the likelihood of collusive attacks. Therefore, we mainly focus on the attacks that could occur within a subchain, especially on block-producing and validator nodes [25].

In a blockchain network, malicious nodes may interfere during the block-producing, validating, and broadcasting phases. For instance, in the block-producing phase, malicious nodes might attempt to generate blocks containing invalid transactions or violating consensus rules. In the validation phase, they might deliberately validate invalid blocks or refuse to validate certain transactions, affecting the network's consistency and security. During the broadcasting phase, malicious nodes could prevent the broadcasting of legitimate blocks or broadcast invalid blocks, causing network forks or inconsistencies.

In the design of this paper, the block-producing phase is completed by specific block-producing nodes, while the validation and broadcasting phases are completed by validator nodes. Therefore, to execute a malicious transaction, collusion between block-producing and validator nodes is required. In the case of a single chain without node sharding, the subchain may be at risk of attack if malicious nodes possess more than 51% of the computing power.

In some blockchain protocols, the main goal of the validation phase is to ensure the validity and consistency of blocks. When the block-producing phase is attacked or contains invalid blocks, the validation phase typically attempts to detect these issues and refuse to accept invalid blocks.

In many blockchain protocols, the main purpose of the validation phase is to ensure the validity and consistency of blocks. Normal validator nodes typically refuse to accept blocks that contain invalid transactions or do not comply with consensus rules. This validation mechanism helps to identify and prevent potential malicious behavior that may occur during the block production phase.

For a subchain with N nodes, let X represent the set of nodes, $\{X_1, \cdots, X_I, \cdots, X_n\}$. F_x denotes the set of malicious nodes within the node set. Without node sharding in a single chain, $P_a = \frac{F_X}{X} > 50\%$ is needed to satisfy an attack condition, meaning at least $\frac{N+1}{2}$ nodes from F_x are required to meet the attack condition. Under the same conditions of N nodes and malicious nodes F_x, now splitting single-chain nodes into block-producing nodes $C_1 = \{C_1, \cdots, C_I, \cdots, C_x\}$ and validator broadcasting nodes $C_2 = \{C_1, \cdots, C_I, \cdots, C_y\}$, where C_1 and C_2 satisfy $C_1 + C_2 = X$, F_{C_1} represents the set of malicious block-producing nodes, F_{C_2} represents the set of malicious validator broadcasting nodes, and they satisfy $F_{C_1} + F_{C_2} = F_X$. At this time, to satisfy a collusion attack between nodes, it is necessary that both $P_b = \frac{F_{C_1}}{C_1} > 50\%$ and $P_c = \frac{F_{C_2}}{C_2} > 50\%$, meaning both F_{C_1} and F_{C_2} need to satisfy the conditions for the number of nodes of $\frac{x+1}{2}$ and $\frac{y+1}{2}$ to meet the attack condition. Here, rounding up $\frac{x+1}{2}$ to satisfy the attack during the block production phase, and rounding down the remaining nodes $\frac{y+1}{2}$ just meets the fifty percent required for an attack during the validator broadcasting phase, considered to meet the attack criteria for the validator broadcasting phase. If the allocation of malicious nodes in the block-producing phase is greater than $\frac{x+1}{2}$, the remaining nodes would not meet the criteria for a collusive attack in the validator broadcasting phase, deeming the attack unsuccessful. Therefore, for a single-chain node sharding to satisfy one collusion attack, the number of malicious nodes in the block-producing phase must be $\frac{x+1}{2}$ (rounded up), and the number of malicious nodes in the validator broadcasting phase must be $X - \frac{x+1}{2}$, with the probability of attack being P_s=$C_{51}^{\frac{x+1}{2}} / C_{100}^{x}$, which is calculated based on the distribution of block-producing nodes, where x is the total number of allocated block-producing nodes and $\frac{x+1}{2}$ is rounded up.

Under the design of this paper, assuming node sharding in a single chain, with the total number of nodes divided into 100 parts, if 51 parts are malicious nodes, then at least collusion between the block-producing and validator broadcasting phases is needed for an attack. The minimum probability of a successful attack can be calculated using the formula P_1=$C_{51}^{\frac{b+1}{2}} / C_{100}^{b}$, with b being the total number of bloc-producing nodes, and the related calculations and results displayed in Figure 4 and Table 2.

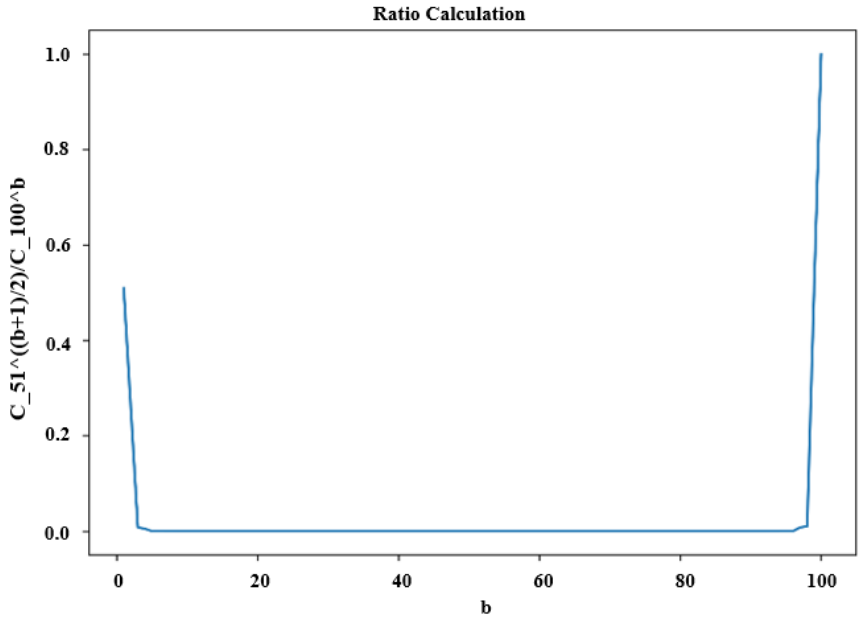

Figure 4. Probability of successful collusion attack in single-chain sharding graph

According to the analysis results of Figure 4 and Table 2, when a single chain is not sharded and malicious nodes occupy 51%, the probability of a collusion attack is 100%. However, when single-chain nodes are divided into block-producing nodes and validator broadcasting nodes, the attack probability shows a curve distribution. When the proportion of block-producing nodes is 1, the probability of attack is 51%. As the proportion of block-producing nodes increases, the attack probability gradually decreases. When the number of block-producing nodes and validator broadcasting nodes each accounts for half of the total number of nodes, the optimal state is reached, and the probability of attack is only 2.46E-15. Compared to an unsharded single chain, this significantly reduces the probability of attack, thereby enhancing security.

Table 2. Data on probability of successful collusion attack in single-chain sharding

1-20	21-40	41-60	61-80	81-100
0.51	2.33E-11	5.69E-15	8.60E-15	9.66E-11
0.257576	2.17E-11	5.52E-15	8.55E-15	9.92E-11
0.007885	6.38E-12	4.09E-15	1.42E-14	4.57E-10
0.005311	5.97E-12	3.99E-15	1.41E-14	4.73E-10
0.000277	1.96E-12	3.20E-15	2.55E-14	2.51E-09
0.00021	1.85E-12	3.12E-15	2.54E-14	2.62E-09
1.56E-05	6.74E-13	2.72E-15	5.01E-14	1.63E-08
1.26E-05	6.38E-13	2.66E-15	5.02E-14	1.71E-08
1.23E-06	2.57E-13	2.51E-15	1.08E-13	1.27E-07
1.04E-06	2.44E-13	2.46E-15	1.09E-13	1.36E-07
1.27E-07	1.08E-13	2.51E-15	2.57E-13	1.23E-06
1.10E-07	1.03E-13	2.46E-15	2.59E-13	1.34E-06
1.63E-08	5.01E-14	2.72E-15	6.74E-13	1.56E-05
1.44E-08	4.80E-14	2.68E-15	6.81E-13	1.75E-05
2.51E-09	2.55E-14	3.20E-15	1.96E-12	0.000277
2.26E-09	2.45E-14	3.16E-15	1.99E-12	0.000325
4.57E-10	1.42E-14	4.09E-15	6.38E-12	0.007885
4.17E-10	1.37E-14	4.05E-15	6.50E-12	0.010303
9.66E-11	8.60E-15	5.69E-15	2.33E-11	0.51
8.89E-11	8.33E-15	5.64E-15	2.38E-11	1

4.2 Cross-Chain Node Sharding Analysis and Comparison

According to the cross-chain validation mechanism designed in this paper, the manufacturer needs to complete the block-producing phase, and the logistics provider must provide some validator nodes for joint validation. Assuming the total network nodes are divided into 100 parts, if there are 51 malicious parts, a complete attack requires collusion between the manufacturer in the block-producing phase and the logistics provider in the cross-chain validation broadcasting phase.

Two possible attack scenarios exist if the manufacturer's block-producing phase is compromised:

(1) Precisely 51% of nodes are malicious: In this scenario, if the malicious nodes in the manufacturer's block-producing phase are exactly 51%, and the remaining malicious nodes suffice for a single-chain node sharding collusion attack.

(2) More than 51% of nodes are malicious: In this scenario, the proportion of malicious nodes in the manufacturer's block-producing phase exceeds 51%, satisfying the conditions for an attack during joint validation with the logistics provider.

Scenario 1: Assume that in the block-producing phase of the manufacturer, malicious nodes just happen to account for 51%, and the remaining number of malicious nodes is only enough to satisfy a collusion attack in single-chain node sharding, with the logistics provider's node situation being identical to that of the manufacturer's. To implement a cross-chain collusion attack, it requires the validator broadcasting nodes of the logistics provider to supplement the remaining malicious nodes.In the subchain manufacturer, the minimum probability of completing an attack is P_1=$C_{51}^{\frac{b+1}{2}}/C_{100}^{b}$,which includes 51% of malicious nodes in the block-producing phase and 50% in the validation phase. After merging the validator broadcasting nodes, their total number is the sum of the manufacturer's validator broadcasting nodes and the logistics provider's validator broadcasting nodes, meeting the attack needs in the validation broadcasting phase requires

$$\frac{\mathrm{Manufacturer's\,Validator\,Broadcasting\,Malicious\,Nodes} + \mathrm{Logistics\,Provider's\,Validator\,Broadcasting\,Malicious\,Nodes}}{Total\ Number\ of\ Validator\ Broadcasting\ Nodes} > 50\%$$

at this time,

$$\frac{\text{Logistics Provider's Validator Broadcasting Malicious Nodes}}{Total\ Number\ of\ Logistics\ Provider's\ Validator\ Broadcasting\ Nodes} > 50\%$$

is required; to ensure the collusion attack in the block-producing phase of the logistics provider, it must satisfy

$$\frac{\text{Logistics Provider's Validator Broadcasting Malicious Nodes}}{Total\ Number\ of\ Logistics\ Provider's\ Validator\ Broadcasting\ Nodes} = 50\%.$$

Therefore, the probability of successfully implementing a cross-chain collusion attack can be calculated using the following formula: P_2=$C_{51}^{\frac{b+1}{2}}/C_{100}^{b} * C_{51}^{\frac{c+1}{2}}/C_{100}^{c}$ (where b is the number of block-producing nodes of the manufacturer, and c is the number of block-producing nodes of the logistics provider). This formula indicates that, with 51% of malicious nodes during the manufacturer's block-producing phase, the logistics provider's validator broadcasting nodes also need a sufficient number of malicious nodes to carry out the collusion attack. The probability P_2 calculates the success rate of the attack in this scenario, considering the joint probability of two independent events (the manufacturer's block-producing phase and the logistics provider's validator broadcasting phase).

From the data in Table 2, it can be observed that the probability of collusion attack with single-chain node sharding $P_1 = C_{51}^{\frac{b+1}{2}}/C_{100}^{b} < 1$. In Scenario 1, $P_2 = C_{51}^{\frac{b+1}{2}}/C_{100}^{b} * C_{51}^{\frac{c+1}{2}}/C_{100}^{c} < P_1 = C_{51}^{\frac{b+1}{2}}/C_{100}^{b} < 1$, since the probability is always less than the original probability (when the probability is less than 1), thus $P_2 < P_1$, meaning the probability of cross-chain collusion attacks is lower than that of single-chain node sharding collusion attacks. The related calculations and results are shown in Figure 5 and Table 3.

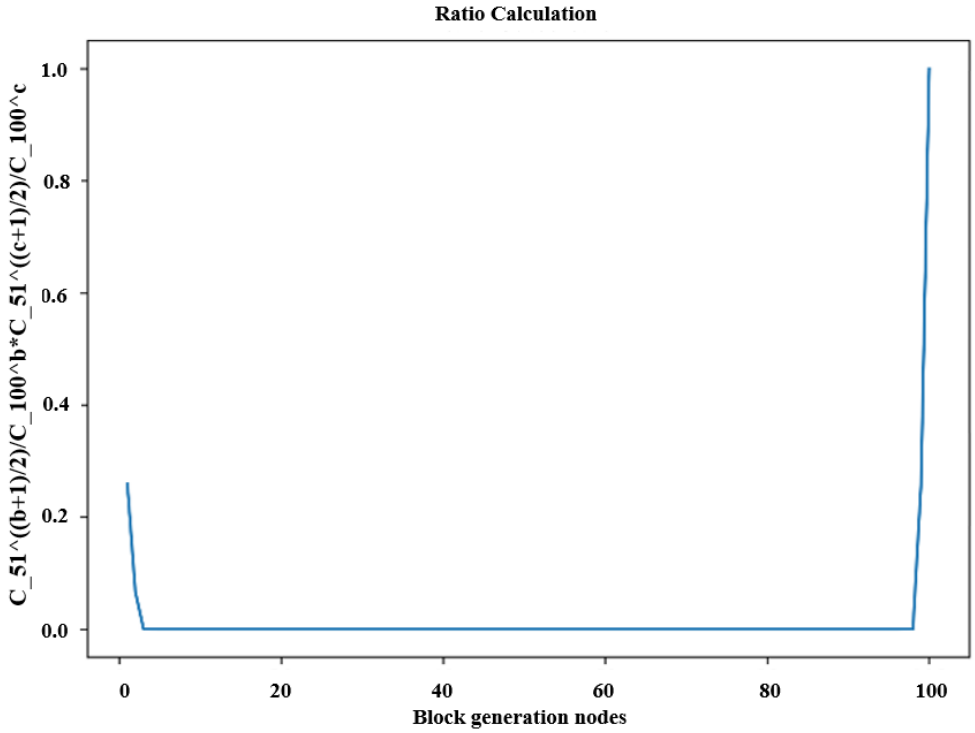

Figure 5. Probability of successful cross-chain sharding collusion attack graph

These figures indicate that in the parallel multichain blockchain model designed in this paper, even in the presence of malicious nodes, the likelihood of a successful cross-chain collusion attack is relatively low, especially compared to the single-chain sharding model. This lower probability of attack, similar to the single-chain cross-chain model, follows a curve distribution. When the number of block-producing nodes from the manufacturer and validator broadcasting nodes from the logistics provider each constitutes half of their respective subchain's total nodes, the optimal state is achieved with an attack probability of only 6.04E-30. This significantly enhances network security, reduces potential risks, and makes the entire system more robust and reliable.

Scenario 2: If the proportion of malicious nodes in the block-producing phase of the manufacturer exceeds 51%, and the remaining number of malicious nodes leads to a collusion attack robability $P_Z = \frac{51-\frac{b+1}{2}}{100-b} < 50\%$ for single-chain sharding, it is insufficient to independently complete a collusion attack within single-chain node sharding. At this time, implementing a cross-chain collusion attack would require the validator broadcasting nodes of the logistics provider to supplement the remaining malicious nodes. According to the model designed in this paper, each chain has at least 51% malicious nodes, meaning the validator broadcasting phase of the logistics provider could provide enough malicious nodes to support the previous transaction's collusion attack.

Table 3. Data on probability of successful cross-chain sharding collusion attack

1-20	21-40	41-60	61-80	81-100
0.2601	5.44E-22	3.24E-29	7.40E-29	9.32E-21
0.066345	4.69E-22	3.05E-29	7.30E-29	9.84E-21
6.22E-05	4.08E-23	1.68E-29	2.01E-28	2.09E-19
2.82E-05	3.56E-23	1.59E-29	1.99E-28	2.24E-19
7.65E-08	3.86E-24	1.03E-29	6.49E-28	6.32E-18
4.39E-08	3.41E-24	9.77E-30	6.47E-28	6.87E-18
2.44E-10	4.55E-25	7.40E-30	2.51E-27	2.65E-16
1.59E-10	4.07E-25	7.08E-30	2.52E-27	2.94E-16
1.52E-12	6.60E-26	6.28E-30	1.17E-26	1.62E-14
1.08E-12	5.97E-26	6.04E-30	1.18E-26	1.84E-14
1.62E-14	1.17E-26	6.28E-30	6.60E-26	1.52E-12
1.21E-14	1.07E-26	6.07E-30	6.69E-26	1.80E-12
2.65E-16	2.51E-27	7.40E-30	4.55E-25	2.44E-10
2.08E-16	2.31E-27	7.17E-30	4.63E-25	3.05E-10
6.32E-18	6.49E-28	1.03E-29	3.86E-24	7.65E-08
5.11E-18	6.01E-28	9.99E-30	3.96E-24	1.06E-07
2.09E-19	2.01E-28	1.68E-29	4.08E-23	6.22E-05
1.74E-19	1.87E-28	1.64E-29	4.22E-23	0.000106
9.32E-21	7.40E-29	3.24E-29	5.44E-22	0.2601
7.90E-21	6.93E-29	3.18E-29	5.68E-22	1

For subchains of manufacturers and logistics providers, both with a total node count of N, let X_a and X_b denote the node sets of manufacturers and logistics providers, X_a=$\{X_1, \cdots, X_I, \cdots, X_n\}$, X_b=$\{X_1, \cdots, X_I, \cdots, X_n\}$; F_a and F_b represent the sets of malicious nodes within the manufacturer's and logistics provider's node sets, respectively. Dividing manufacturer nodes into block-producing nodes $C_a = \{C_1, \cdots, C_I, \cdots, C_x\}$ and validator broadcasting nodes $C_b = \{C_1, \cdots, C_I, \cdots, C_y\}$, C_a and C_b satisfy $C_a + C_b$=X_a; F_{C_a}represents malicious block-producing nodes, and F_{C_b} represents malicious validator broadcasting nodes, satisfying $F_{C_1} + F_{C_2} = F_a$. In scenario 2, $P_{21} = \frac{F_{C_a}}{C_a} > 51\%$ and $P_{22} = \frac{F_{C_b}}{C_b} < 50\%$. Thus, block production phase attacks are successful, while validator broadcasting phase attacks in single-chain sharding are not, necessitating supplementary malicious nodes from the logistics provider to satisfy collusion. Dividing logistics provider nodes into block-producing nodes $C_c = \{C_1, \cdots, C_I, \cdots, C_x\}$ and validator broadcasting nodes $C_d = \{C_1, \cdots, C_I, \cdots, C_y\}$, C_c and C_d satisfy $C_a + C_b$=X_b; F_{C_c} reesents malicious block-producing nodes, and F_{C_d} represents malicious validator broadcasting nodes, satisfying $F_{C_c} + F_{C_d} = F_b$. The logistics provider's validator broadcasting nodes need to satisfy $P_{he} = \frac{F_{C_d} + F_{C_b}}{C_b + C_d} > 50\%$. Since $P_{22} = \frac{F_{C_b}}{C_b} < 50\%$, $P_{32} = \frac{F_{C_d}}{C_d} > 51\%$, at this time, $P_{31} = \frac{F_{C_c}}{C_c} < 50\%$, indicating that after receiving data from the manufacturer, the logistics provider internally lacks enough malicious nodes to complete a collusion attack.

In this scenario, since the logistics provider has already contributed a significant number of malicious nodes in a previous validator broadcasting, gathering enough malicious nodes for another collusion attack in the subsequent block-producing phase is challenging. This may lead to errors in the block-producing phase, resulting in failed subsequent transactions.

In summary, scenario 2 highlights a crucial security consideration: even if a collusion attack is successfully executed in one transaction, maintaining such an attack state in closed-loop transactions is challenging. As transactions progress, attackers need to continuously maintain a sufficient number of malicious nodes, which is difficult in practice, thereby enhancing the overall security of the system.

The cross-chain validation mechanism is an effective solution to the scalability issue of single blockchain networks. By connecting multiple blockchain networks, it not only distributes data load and traffic but also significantly enhances the entire system's throughput and performance. The core of this method is distributing the validation process across different blockchain networks, achieving a higher degree of security and decentralization.

Through cross-chain validation, the risk of single blockchain networks becoming targets of attacks or suffering from single points of failure is reduced. This dispersed validation framework greatly strengthens the overall system's robustness and security. Moreover, cross-chain validation ensures the consistency and trustworthiness of transactions and operations across different blockchain networks, which is crucial for maintaining the integrity of the blockchain ecosystem.

5 Conclusion and Outlook

This paper delves into managing data related to "Dual Carbon" goals (carbon peak and carbon neutrality) using blockchain technology and proposes a high-performance carbon cycle supply chain data sharing method based on a parallel multichain blockchain architecture. By constructing an interactive "child/parent" chain structure and implementing shard processing, it not only facilitates cross-chain access and effective sharing of carbon data but also significantly enhances the overall data processing capability. While achieving carbon data sharing, it optimizes the consortium chain structure by dividing the consortium chain into

multiple relay chains, and further splitting relay chains into numerous private chains, increasing the granularity of sharding by a 2n ratio. These parallel-running subchains improve the system's overall throughput, thus addressing the issues of information silos and the insufficient throughput inherent in traditional single-chain structures.

To optimize the security issues in the traditional single-chain mode, especially the typical 51% attack, this paper designs a dynamic node mechanism. By implementing subchain cross-chain node sharding, nodes are refined into block-producing nodes and validator broadcasting nodes. Such division of labor allows transactions to be processed in parallel on multiple nodes, significantly increasing system throughput. Furthermore, the security analysis comparison between single-chain sharding and cross-chain sharding reveals that cross-chain sharding offers a more significant improvement in system security. This is because cross-chain sharding enhances security by dispersing risks and increasing the cost of attacks. Specifically, even if attackers successfully compromise part of the system, the entire system will not collapse due to the independence of other parts. Additionally, since transactions are continuous, if an attack leads to incorrect transactions, subsequent transactions unable to meet the attack conditions will interrupt the transaction, thus greatly reducing the overall risk.

The scheme thoughtfully considers the heterogeneity of participants in the carbon market scenario and constructs a high-performance data sharing and processing framework suitable for the carbon market by designing interaction rules between chains. This has significant implications for advancing the application of blockchain technology in achieving "Dual Carbon" goals. It not only provides robust technical support for key aspects such as carbon emission statistics, monitoring, reporting, and trading but also facilitates low-carbon transformation.

Future research will focus on in-depth exploration of cross-chain node sharding technology. This technology divides nodes into block-producing nodes and validator broadcasting nodes, and due to the temporal differences in processing between the two, parallel conflicts may arise. Therefore, we need to study how to reasonably allocate the number of nodes and adjust delay times to optimize overall network performance and ensure the system's efficiency and stability. This will include improvements to existing algorithms and the proposal and testing of new algorithms to achieve more efficient node management and resource allocation strategies.

Data Availability

The data used to support the research findings are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.

[2] P. Chen, L. Zhiqiang, L. Zhen, and L. Yu, "Research on blockchain scalability: Issues and methods," *Comput. Res. Dev.*, vol. 55, no. 10, pp. 2099–2110, 2018. https://doi.org/10.7544/issn1000-1239.2018.20180440

[3] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and S. Prateek, "A secure sharding protocol for open blockchains," in *CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria*, 2016, pp. 17–30. https://doi.org/10.1145/2976749.2978389

[4] H. Dang, T. T. A. Dinh, D. Loghin, E. C. Chang, Q. Lin, and B. Chin Ooi, "Towards scaling blockchain systems via sharding," in *SIGMOD '19: Proceedings of the 2019 International Conference on Management of Data, Amsterdam, Netherlands*, 2019, pp. 123–140. https://doi.org/10.1145/3299869.3319889

[5] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: Scaling blockchain via full sharding," in *CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada*, 2018, pp. 931–948. https://doi.org/10.1145/3243734.3243853

[6] M. Cortes-Goicoechea, L. Franceschini, and L. Bautista-Gomez, "Resource analysis of ethereum 2.0 clients," in *Conference on Blockchain Research & Applications for Innovative Networks and Services, Berlin, Germany*, 2021, pp. 1–8. https://doi.org/10.1109/BRAINS52497.2021.9569812

[7] F. Cassez, J. Fuller, and A. Asgaonkar, "Formal verification of the ethereum 2.0 beacon chain," in *Tools and Algorithms for the Construction and Analysis of Systems. TACAS 2022. Lecture Notes in Computer Science*. Springer, Cham., 2022, pp. 167–182. https://doi.org/10.1007/978-3-030-99524-9_9

[8] J. Kwon and E. Buchman, "A network of distributed ledgers," 2018. https://cosmos.network/whitepaper

[9] S. He, X. Huang, and X. Chen, "A review of research on the development and application of blockchain cross-chain technology," *J. Xihua Univ. (Nat. Sci. Ed.)*, vol. 40, no. 3, pp. 1–14, 2021. https://doi.org/10.12198/j.issn.1673-159X.3845

[10] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016. https://lightning.network/lightning-network-paper.pdf

[11] A. Miller, I. Bentov, S. Bakshi, R. Kumaresan, and P. McCorry, "Sprites and state channels: Payment networks that go faster than lightning," in *Financial Cryptography and Data Security. FC 2019. Lecture Notes in Computer Science*. Springer, Cham., 2019. https://doi.org/10.1007/978-3-030-32101-7_30

[12] C. Pan, S. Tang, Z. Ge, Z. Q. Liu, Y. Long, Z. Liu, and D. Gu, "Gnocchi: Multiplexed payment channels for cryptocurrencies," in *Network and System Security. NSS 2019. Lecture Notes in Computer Science*. Springer, Cham., 2019, pp. 488–503. https://doi.org/10.1007/978-3-030-36938-5_30

[13] M. Borkowski, P. Frauenthaler, M. Sigwart, and T. Hukkinen, "Cross-blockchain technologies: Review, state of the art, and outlook," 2019. https://doi.org/10.13140/RG.2.2.30902.14403

[14] H. Chen and Y. Wang, "Sschain: A full sharding protocol for public blockchain without data migration overhead," *Pervasive Mob. Comput.*, vol. 59, p. 101055, 2019. https://doi.org/10.1016/j.pmcj.2019.101055

[15] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," 2016. https://polkadot.network/PolkaDotPaper.pdf

[16] R. Wang, W. T. Tsai, J. He, C. Liu, and E. Deng, "A distributed digital asset-trading platform based on permissioned blockchains," in *Smart Blockchain. SmartBlock 2018. Lecture Notes in Computer Science*. Springer, Cham., 2018, pp. 55–65. https://doi.org/10.1007/978-3-030-05764-0_6

[17] J. Wang, J. Huang, L. Kong, G. Chen, D. Zhou, and J. J. P. C. Rodrigues, "A privacy-preserving vehicular data sharing framework atop multi-sharding blockchain," in *2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain*, 2021, pp. 1–6. https://doi.org/10.1109/GLOBECOM46510.2021.9685366

[18] S. Lin, Y. Kong, and S. Nie, "Overview of block chain cross chain technology," in *2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Beihai, China*, 2021, pp. 357–360. https://doi.org/10.1109/ICMTMA52658.2021.00083

[19] A. A. Yazdeen, S. R. M. Zeebaree, M. M. Sadeeq, S. F. Kak, O. M. Ahmaed, and R. R. Zebari, "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review," *Qubahan Acad. J.*, vol. 1, no. 2, pp. 8–16, 2021. https://doi.org/10.48161/qaj.v1n2a38

[20] M. Westerkamp and J. Eberhardt, "Zkrelay: Facilitating sidechains using zksnark-based chain-relays," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy*, 2020, pp. 378–386. https://doi.org/10.1109/EuroSPW51379.2020.00058

[21] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Anoud Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Netw. Appl.*, vol. 14, pp. 2901–2925, 2021. https://doi.org/10.1007/s12083-021-01127-0

[22] Y. Abuidris, C. Wang, and W. Yang, "Collaborative multi-chain architecture for data transmission across homogeneous blockchain," in *2022 International Conference on Innovations and Development of Information Technologies and Robotics (IDITR), Chengdu, China*, 2022, pp. 105–110. https://doi.org/10.1109/IDITR54676.2022.9796483

[23] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," *Applied Sciences*, vol. 11, no. 20, p. 9372, 2021. https://doi.org/10.3390/app11209372

[24] M. Saad, J. Spaulding, L. Njilla, C. A. Kamhoua, S. S. Shetty, D. Nyang, and D. A. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1977–2008, 2020. https://doi.org/10.1109/COMST.2020.2975999

[25] C. Huang, Z. Wang, H. Chen, Q. Hu, Q. Zhang, W. Wang, and X. Guan, "Repchain: A reputation-based secure, fast, and high incentive blockchain system via sharding," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4291–4304, 2020. https://doi.org/10.1109/JIOT.2020.3028449