Cross-Domain Data Compliance Flow Mechanisms: A Robust Sidechain and Relay Chain Integration Approach in Blockchain

Sheng Peng[1,a], Qiuling Feng[2, b], Di Sun[3, *], Linkai Zhu[2, c], Siyu Chen[4,d], Jiayun Wang[4, e]

[a] Email: saint_peng@qq.com

[b] Email: f3497851037@126.com

*Corresponding author emai1: 2018010926@sjzpt.edu.cn

[c] Email: linkai@hueb.edu.cn

[d] Email: siyu121451@gmail.com

[e] Email: 2151355700@qq.com

[1]Academy of Management, Guangdong University of Science and Technology, Dongguan, China

[2]Information Technology School, Hebei University of Economics and Business, Shijiazhuang, China

[3]Department of Information Engineering, Shijiazhuang College of Applied Technology, Shijiazhuang, China

[4]International Education School, Hebei University of Economics and Business, Shijiazhuang, China

Abstract—In response to the challenges of cross-domain data compliance circulation across various trust domains and ensuring the cross-domain exchange of private data, this study constructs a cross-domain data compliance flow model combining sidechain and relay chain utilizing blockchain technology. Initially, the structure of the sidechain and relay chain is established, followed by proposing an architectural model for cross-domain data circulation based on these chains. The model integrates a cross-domain access mechanism designed around smart contracts, leveraging the strengths of blockchain's decentralized nature. This allows for secure and efficient cross-domain data transfers while ensuring compliance and integrity throughout the process. By addressing the inherent complexities and security concerns of cross-domain data exchanges, this model represents a significant advancement in blockchain applications, promising to facilitate robust, compliant, and efficient data exchanges across various trust domains.

Keywords-Blockchain; Relay Chain; Data Exchange; Cross-Domain

ICBBEM 2024, March 29-31, Wuhan, People's Republic of China

DOI 10.4108/eai.29-3-2024.2347324

1 Introduction

With the rapid development of blockchain technology and the thriving digital economy, blockchain infrastructure is undergoing profound evolution. Various chain structures like public chains, sidechains, relay chains, permissioned chains, and consortium chains are emerging, offering diverse technological choices for data storage in the blockchain ecosystem and data exchange. Driven by the digital economy, user transaction data is experiencing explosive growth, raising new challenges for the compliance and security of data circulation.

However, technical differences and competitive relations between different blockchain ecosystems lead to the "island effect" of data, where user assets and application data are difficult to seamlessly exchange between different chains, limiting the free flow of data. To break this "island effect" and make more effective use of data resources, promoting cross-domain and cross-department cooperation, we urgently need a service model for cross-domain data compliant flow to enhance the efficient circulation of business and value in blockchain projects.

In dealing with vast transaction data, data security becomes an urgent issue to address in cross-domain data exchange. Current cross-domain models focus on cloud computing and online social networking environments but essentially still model data control within a single domain, usually managed by a centralized authority for access control decisions. This raises concerns about the trustworthiness of single entities, making data security an issue that cannot be overlooked.

The original blockchain networks, such as Bitcoin and Ethereum, face challenges in handling a large volume of data exchanges and complex smart contracts due to factors like consensus mechanisms, block size, and block generation time, resulting in slow transaction speeds, low efficiency, high transaction costs, and interoperability issues. As blockchain technology continues to evolve and application scenarios expand, these problems become more pronounced. To address these issues, researchers are considering integrating sidechains and relay chains into the blockchain ecosystem.

Therefore, to promote the security and efficiency of cross-domain data exchange in the blockchain field, this article proposes a cross-domain data compliant flow model based on the combination of sidechains and relay chains. By constructing a network model of relay chain and sidechain blockchain structures, intra-domain resource data can be accessed mutually through sidechains. Meanwhile, the main chain acts as a trusted certification platform, responsible for data storage and compliance verification of incoming data. This combined model of sidechains and relay chains theoretically enables unlimited expansion, effectively mitigating the issue of high storage overhead and resolving system stability bottlenecks. This model is expected to enhance the security and efficiency of cross-domain data exchanges in the blockchain domain.

2 Related work

Blockchain, as a distributed ledger used to record transactions and track assets, is widely applied to the decentralized infrastructure of emerging digital cryptocurrencies. With the

increasing popularity of cryptocurrencies, Study [1] elaborates the basic principles, technologies, methods, and current research status of blockchain and related Bitcoin, introducing the future development trend of a parallel society based on blockchain.

Work [2] designs a cross-domain data sharing model architecture based on a master-slave chain and devises a cross-domain access mechanism for smart contracts, achieving secure sharing of private data across domains. Literature [3] introduces the concept of blockchain interoperability, designing cross-chain operational models through inter-chain, inter-layer, inter-fork, inter-slice, on-chain, and off-chain interoperability, exploring the development trends of blockchain interoperability and cross-chain technology. Literature [4] designs a blockchain certificate, utilizing consortium chain's distributed ledger to store and verify blockchain certificates, achieving identity verification and cross-domain authentication of domain trust entities. Literature [5] proposes a deterministic fair contract signing protocol based on blockchain, establishing multi-party trust relationships among participating nodes, ensuring fairness, privacy, and dynamic management of multi-party contracts.

As blockchain technology rapidly evolves, cross-chain interaction has become one of the important means of data exchange, expanding blockchain applications. Current mainstream cross-chain blockchain technology solutions are mainly: notary mechanisms, hash locking, and distributed private key control. The most famous cross-chain projects currently are Cosmos and Polkadot [6], both adopting a multi-chain, multi-layer architecture based on relay chains. Sidechain and relay chain models have their distinct advantages and disadvantages in implementing data exchanges on the chain, with high application value in asset transfer and information interaction, indicating that sidechain and relay chain technologies will be the main force in future cross-chain technology. Literature [7] improves cross-chain security by applying TEE technology in the sidechain or relay chain model with non-interactive zero-knowledge proofs.

Blockchain, as a decentralized and distributed technology, offers new solutions for enabling compliant cross-domain data circulation. In a distributed environment, local servers, to meet local demands, form relatively independent trust application domains. However, a single trust application domain is often insufficient to meet user needs, necessitating the implementation of data circulation across multiple trust application domains. To address this issue, a framework combining sidechains and relay chains is proposed. To overcome these drawbacks and enhance blockchain performance to meet the needs of cross-domain data circulation, this article proposes a cross-domain data compliant flow model based on the combination of blockchain sidechains and relay chains, using sidechain technology to alleviate the pressure of information storage on the main chain, enhance the scalability of the main chain, and use the combined network solution of relay chains to solve the problem of cross-domain data transmission, achieving compliant data flow on the blockchain.

Regarding the security issues of extensive data interaction in blockchain networks, literature [8] utilizes blockchain in the domain of inter-domain routing security, conducting research on inter-domain routing authentication, intelligent management, and DDoS defense.

3 Cross-Domain Data Compliance Flow Model Combining Sidechain and Relay Chain

3.1 System Architecture Design Combining Sidechain and Relay Chain

3.1.1 Structural Design of Combining Sidechain and Relay Chain

Our scheme classifies nodes involved in different data exchange processes into main chain nodes, sidechain nodes, and relay chain nodes, according to the different functions of various chains.

Main chain nodes: They are primarily responsible for the storage of transaction data. These nodes connect to the relay chain network through sidechain nodes and are tasked with providing data for exchange with other main chains. Data exchanges occur between main chain nodes and sidechain nodes, where compliance smart contracts on the main chain execute data validation and compliance auditing to ensure the legality and compliance of incoming cross-chain data.

Sidechain nodes: These nodes, consistent with main chain nodes, mainly generate cross-chain transaction requests and invoke the main chain's KPIs to monitor and validate main chain data. They process and validate local data, create corresponding tokens, and submit data for exchange to the relay node network.

Relay chain nodes: They are chiefly responsible for executing consensus mechanisms to verify the validity of transactions, generating corresponding cross-chain blocks, and implementing asset transfer and information interaction based on routing forwarding strategies, thus completing the trans-domain transmission of assets.

Given the geographical diversity of transaction data generation, relay chain nodes are distributed appropriately across different regions. Acting as a bridge for the main sidechain nodes of each domain, relay chain nodes enable the exchange of data between domains.

3.1.2 Architectural Design of Data Exchange Model Based on Sidechain-Relay Chain Structure

Given operational requirements, sidechain data must maintain consistency with main chain data and implement data exchange by processing main chain data through a "bi-directional anchoring" mechanism.

A sidechain is an independent blockchain system. When a user initiates a transaction on the main chain, the encrypted currency is sent to a specific anchoring address, completing the locking and recording. This contract will monitor changes in the anchoring address. Once the main chain assets are locked, the corresponding assets on the sidechain will be generated or unlocked, allowing for the interaction of assets to be transferred on the sidechain. The sidechain network confirms to ensure that operations are correctly executed on the sidechain.

Different nodes in different trust domains perform various functions and apply blockchain technology differently to achieve cross-domain data exchange. Drawing on the principles of

packet switching in computer networks, we link important sidechain and relay chain nodes within each data domain to facilitate data interaction across different trust domains. The architectural design diagram in Figure 1 for the data exchange model based on the combination of sidechain and relay chain designed as follows:

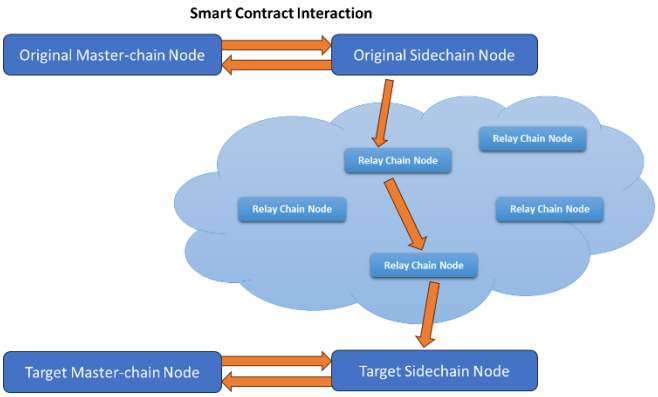

Figure 1. Data exchange process in cross-chain.

The data exchange process begins when a user initiates a transaction on the main chain, aiming to transfer assets, execute smart contracts, or carry out other cross-chain operations between different blockchains. In the transaction initiated on the main chain, the involved assets are locked into a specific anchoring address. This means that the user's assets on the main chain are locked, waiting for subsequent processing. Once the transaction on the main chain is confirmed and the assets are anchored, related smart contracts or mechanisms will trigger the corresponding operations on the sidechain. This may include unlocking the corresponding assets on the sidechain for processing. After the sidechain receives the trigger signal, the corresponding smart contract or logic will be executed, which may involve processing data, changing states, executing business logic, etc. The sidechain's processing ensures the compliance and consistency of cross-chain data. After the sidechain has processed the user's request, it needs to generate proof that the operation on the sidechain has been completed and is legitimate and valid. This could be a digital signature, a hash value, or some other form of evidence. This proof will be submitted to the relay chain as confirmation of the cross-chain operation, which can be achieved through the routing forwarding mechanism on the relay chain. The relay nodes on the relay chain receive the proof and confirm that the operation on the sidechain has been completed. The relay nodes on the relay chain, according to the asset information query forwarding table, facilitate the transfer of assets to the target blockchain for data interaction, forwarding the asset change information from the original chain sidechain to the target node sidechain. This step ensures the reliability and compliance of the cross-chain operation. After confirmation by the relay chain, the assets locked on the main chain will be unlocked, and the user's transaction on the main chain will be completed. This means the entire cross-chain process has been successful, and assets have flowed compliantly between different chains. The Cross chain data exchange algorithm as show below in Algorithm 1:

Algorithm 1 CrossChainDataExchange Algorithm

Input: $T_{main}(A_u)$ ▷ Transaction on the main chain with assets A_u
Output: Transaction completion status and A_{final}
Main Chain Processing:
Lock A_u at $Addr_{anchor}$ ▷ Lock Assets
Await confirmation of T_{main} ▷ Await Confirmation
Trigger Sidechain Operations:
if confirmed **then**
    Execute C_{sc} yielding Op_{side} ▷ Execute smart contracts
end if
Sidechain Operations:
for each operation in Op_{side} **do**
    Execute operation
    Check state and business logic
end for
Generate P_{proof} of operations ▷ Proof Generation
Submit P_{proof} to R_{relay} ▷ Submit to Relay Chain
Relay Chain and Verification:
if $V_{verify}(P_{proof})$ successful **then**
    Initiate asset transfer and update states
    Unlock A_u to A_{final}
else
    Handle verification failure
end if
if not confirmed **then**
    Handle transaction failure
end if

3.2 Design of Sidechain Access Mechanism Based on Smart Contracts

3.2.1 Access Algorithm

The data interaction and asset transfer between the sidechain and the main chain are realized through smart contracts. The main chain needs to deploy smart contracts, including logic and rules related to sidechain access, and define how to communicate with the sidechain. The main chain and sidechain use "bi-directional anchoring" to maintain data consistency. By anchoring specific data or states on the main chain, the sidechain can obtain, verify, and acquire relevant information. This is achieved by storing certain information from the main chain, such as hash values or other identifiers, into the sidechain. When trigger conditions are met, the smart contract on the main chain can initiate specific events on the sidechain. Upon receiving a request from the main chain, the sidechain conducts data verification to ensure data integrity and compliance.

3.2.2 Security Analysis

Security of smart contracts: Smart contracts on the main chain should undergo thorough security audits and testing to prevent potential vulnerabilities and attacks. Contracts should follow best practices, including secure coding standards, avoiding reentrancy attacks, and protecting against overflow, etc.

Security of the anchoring mechanism: Hash encryption technology is used to ensure the integrity and verifiability of the anchored information.

Cross-chain communication security: Communication between the main chain and the sidechain uses secure HTTPS protocols and encryption technologies to prevent information leakage, man-in-the-middle attacks, and tampering.

Permission and access control: Smart contracts and sidechains should implement appropriate permissions and access controls to limit access to critical system functions. Only authorized entities should be able to perform specific operations.

Data verification and consistency: The sidechain needs effective mechanisms to verify data received from the main chain to ensure its integrity and legality. Consistency algorithms ensure that the state between the main chain and the sidechain remains synchronized.

3.3 Inter-Domain Data Exchange Mechanism Based on Routing Forwarding

3.3.1 Exchange Mechanism

This study designs an inter-domain data exchange mechanism based on routing forwarding to construct the asset forwarding function of the relay chain network. Each blockchain trust domain can be analogized to an autonomous system, with the relay chain acting as a router between blockchains. Each blockchain maintains a blockchain routing table, which contains information for inter-domain cooperation such as public keys, blockchain address mappings, cooperation protocols, etc. It also introduces the inter-domain protocol for exchanging relay chain information between different routers, determining the best forwarding path to the target chain. Similar to traditional routers, the inter-domain routing protocol can regularly update the blockchain routing table to adapt to the dynamic blockchain network. Data exchange and verification between different relay chain nodes are implemented through smart contracts. Digital signature security mechanisms ensure the security and confidentiality of inter-domain data exchange.

3.3.2 Security Analysis

Identity authentication: Ensure that blockchain relay chain nodes can effectively verify the identity of other nodes to prevent identity forgery or deception.

Data encryption: Use encryption algorithms during data transmission to ensure data confidentiality and prevent unauthorized access and eavesdropping.

Access control: Restrict access to router functions, allowing only authenticated nodes to execute routing decisions and data forwarding.

Routing table security management: Maintain the routing table with a secure updating mechanism to prevent tampering or insertion of false information.

4 Advanced Privacy and Security Enhancements in Blockchain Systems

4.1 Zero-Knowledge Proofs (ZKPs) Implementation for Data Privacy Assurance

The incorporation of Zero-Knowledge Proofs (ZKPs) into our blockchain model significantly elevates data privacy. ZKPs enable a prover (P) to validate the truth of a claim to a verifier (V)

without revealing any information besides the validity of the claim itself. In our blockchain framework, ZKPs are employed for validating transactions or ensuring data compliance (Comp) without exposing underlying sensitive information (SI). This implementation, denoted as ZKP(P,V,Comp), is vital in environments where maintaining data privacy, such as cross-domain information exchanges, is critical.

4.2 Advanced Data Anonymization Techniques and Access Control Protocols

4.2.1 Implementing Data Anonymization

Our framework adopts robust data anonymization techniques, including data masking, pseudonymization, and aggregation. These methods are applied to modify personal data, ensuring that individuals cannot be readily identified, thereby protecting their privacy. This approach is particularly crucial in blockchain environments where data sharing across different domains is common. By anonymizing data, our system allows for its utilization and analysis while safeguarding individual privacy.

4.2.2 Advanced Access Control Mechanisms

We use access control mechanism called Role-Based Access Control (RBAC) within our blockchain model. These systems define access rights based on user roles, ensuring that only authorized entities can access sensitive data under appropriate conditions.

In addition to implementing RBAC, our framework establishes mechanisms for monitoring and logging access to sensitive data. This includes creating audit trails and implementing real-time monitoring systems to detect unauthorized access attempts promptly. These measures are crucial for maintaining data integrity and confidentiality, reinforcing the trustworthiness and reliability of our blockchain system.

5 Conclusion

The Cross-Domain Data Compliance Flow Model, integrating sidechain and relay chain architectures, represents a significant advancement in blockchain technology, particularly in the realm of secure and efficient data exchange. This model innovatively combines varied node types, bi-directional anchoring, and smart contracts to ensure data integrity and compliance, while also facilitating secure asset transfers across blockchain networks. Its rigorous approach to security analysis and emphasis on scalability not only addresses existing vulnerabilities but also broadens the potential for inter-domain communication. This advancement is pivotal, as it enhances cross-chain interoperability and extends blockchain applicability across diverse digital domains, marking a substantial contribution to the field.

Acknowledgment. This research is supported by Guangdong Philosophy and Social Science Planning Project (GD23SQGL03). It is supported by Science Research Project of Hebei Education Department：(BJK2024111).

References

[1] F. Y. Wang, Y. Yuan, C. Rong, and J. J. Zhang, "Parallel blockchain: An architecture for CPSS-based smart societies," in IEEE Transactions on Computational Social Systems, vol. 5, no. 2, pp. 303-310, 2018.

[2] Y. Liu, X. Xing, Z. Tong, X. Lin, J. Chen, Z. Guan, and W. Susilo, "Secure and Scalable Cross-Domain Data Sharing in Zero-Trust Cloud-Edge-End Environment Based on Sharding Blockchain," in IEEE Transactions on Dependable and Secure Computing, 2023.

[3] Q. Wang, F. Li, X. Ni, L. Xia, G. Liang, and Z. Ma, "Research on Blockchain Interoperability and Cross-Chain Technology," in Journal of Frontiers of Computer Science & Technology, vol. 17, no. 8, pp. 1749, 2023.

[4] S. Budhiraja and R. Rani, "TUDocChain-securing academic certificate digitally on blockchain," in Inventive Computation Technologies 4, Springer International Publishing, pp. 150-160, 2020.

[5] S. Mauw, S. Radomirovic, and M. T. Dashti, "Minimal message complexity of asynchronous multi-party contract signing," in 2009 22nd IEEE Computer Security Foundations Symposium, pp. 13-25, July 2009.

[6] I. Kang, A. Gupta, and O. Seneviratne, "Blockchain Interoperability Landscape," in 2022 IEEE International Conference on Big Data (Big Data), pp. 3191-3200, December 2022.

[7] R. Yin, Z. Yan, X. Liang, H. Xie, and Z. Wan, "A survey on privacy preservation techniques for blockchain interoperability," in Journal of Systems Architecture, vol. 140, 102892, 2023.

[8] E. Zeydan, J. Mangues, S. S. Arslan, and Y. Turk, "Blockchain-based Self-Sovereign Identity for Routing in Inter-Domain Networks," in IEEE Communications Magazine, 2023.