Research on Inter-Chain Resolution and Interoperability Mechanisms Based on Relay Chains

Zewei Zhu[1]

[1]*Yunnan University of Finance and Economics, Information Center, South Campus, Yunnan University of Finance and Economics, Wuhua District, Kunming City, Yunnan Province, China*

Keywords
Domain Name System (DNS); domain name resolution; blockchain-based architecture; decentralized services

Correspondence Email:
202302110719@stu.ynufe.edu.cn

Abstract
The Domain Name System (DNS) has long served as the predominant solution for domain name resolution. However, the existing DNS under a unilateralist framework presents vulnerabilities in security management, which can adversely impact thequality of domain resolution services. Consequently, the development of a highly secure DNS is of paramount importance. To address this issue, we propose a blockchain-based domain name system architecture named RNS, which resolves the unilateralism inherent in traditional DNS through decentralized domain resolution services. We enhance the system's scalabilityby incorporating relay chains.Furthermore, to ensure the security and decentralized characteristics of RNS, we employ Decentralized Identifiers (DID) as the domain identity authentication framework. Experimental results demonstrate that, compared to existing solutions, RNS achieves improved throughputand reduced transaction communication latency, thereby offering an innovative approach that integrates security, high performance, and scalability for applications involving domain resolution in complex network architectures.

1. Introduction

The Domain Name System (DNS) serves as the core infrastructure of the Internet based on a centralized hierarchical architecture, undertaking the crucial task of converting human-readable domain names into computer-recognizable IP addresses. Since its inception in 1983, this hierarchical structure of "root server to top-level domain server (TLD) to authoritative domain server" has supported the expansion of the Internet from a few hosts to billions of devices, becoming the "centralized nerve center" of global network communication. However, the inherent flaws of the centralized architecture are becoming fundamental challenges facing the DNS system. As the Internet evolves from an "elite tool" to a "universal infrastructure," and as users' demands for "security, privacy, and performance" continue to increase, this design of "centralized decision-making and hierarchical control" is revealing increasingly serious structural vulnerabilities.

In 2002, the DNS root server suffered a large-scale DDoS attack, severely affecting global domain name

resolution services. In 2014, a DNS resolution failure occurred in China, resulting in varying degrees of DNS pollution for all generic domains. In 2015, the national top-level domain of Türkiye was attacked, making almost all (.TR) domains inaccessible. In 2016, hackers launched a large-scale DDoS attack on the centralized DNS service provider Dyn, causing dozens of t o p websites such as Twitter, Netflix, and Spotify to become inaccessible, affecting tens of millions of users [1], [2]. To address the inherent flaws of the IP system and its inability to adapt to content-centric, high-speed mobile, IoT, and industrial internet business needs, various new network system solutions have been proposed by the industry and academia. In 2010, the National Science Foundation of the United States funded four Future Internet Architecture (FIA) projects [3]. Among them, the Named Data Networking project aims to develop and establish a content-centric new network architecture [4]. However, due to its disruptive architecture, operators still encounter many challenges in practical deployment, and it fails to fundamentally solve the unilateralism problem existing in the DNS system.

Since Satoshi Nakamoto introduced the Bitcoin system [2], blockchain technology has experienced rapid development, with its applications expanding to various fields. Research on utilizing blockchain for DNS is one such aspect. In this regard, Wang Jingyi proposed the Blockchain Naming System (BNS), which, on the basis of enhancing the fundamental functions of DNS, introduces new features such as chain resolution and node/wallet user resolution. However, the current related systems face the following issues: 1) resolving the domain name of the peer for interoperation, and 2) packaging the resolution results and interoperation information into messages and sending them to the cross-chain relay for cross-chain communication. The solution proposed by BNS is to separate these two operations, allowing users to perform them step by step. Although this simplifies the complexity of the system, it significantly increases the inconvenience for users.

In this article, we introduce the Relay-Chained Blockchain Naming System (RNS). A highlight of our contribution in practical usage scenarios lies in the construction of an innovative domain name resolution architecture. This architecture incorporates cross-chain interoperability state nodes and domain name registration and resolution state nodes to address the aforementioned issue, enabling users to initiate cross-chain transactions without needing to concern themselves with the intricacies of domain name resolution. The domain name registration and resolution state nodes handle DID registration and DID documents storage transactions, and assist the cross-chain interoperability state nodes in domain name resolution during cross-chain interoperability. The cross-chain interoperability state nodes process cross-chain interoperability requests and collaborate with the domain name registration and resolution state nodes to perform domain name resolution, transaction verification and synchronization, and complete cross-chain transactions. This relay chain architecture not only addresses the issue of domain name resolution but also provides an efficient solution for cross-chain communication among users on different chains.

2. Research Methods

a. Overview of system model

Figure 1 illustrates the system model, with the core being the relay chain layer. The relay chain layer is responsible for consensus, state maintenance, cross-chain coordination, and the direct storage of DID and DID documents. The heterogeneous chains in the upper and lower parts of the figure are not internal

layers of the system, but external arbitrary blockchain networks, used to demonstrate the bridging role of RNS in relay domain name resolution and interoperability. These heterogeneous chains can be any compatible blockchain, achieving seamless interaction through the relay chain.

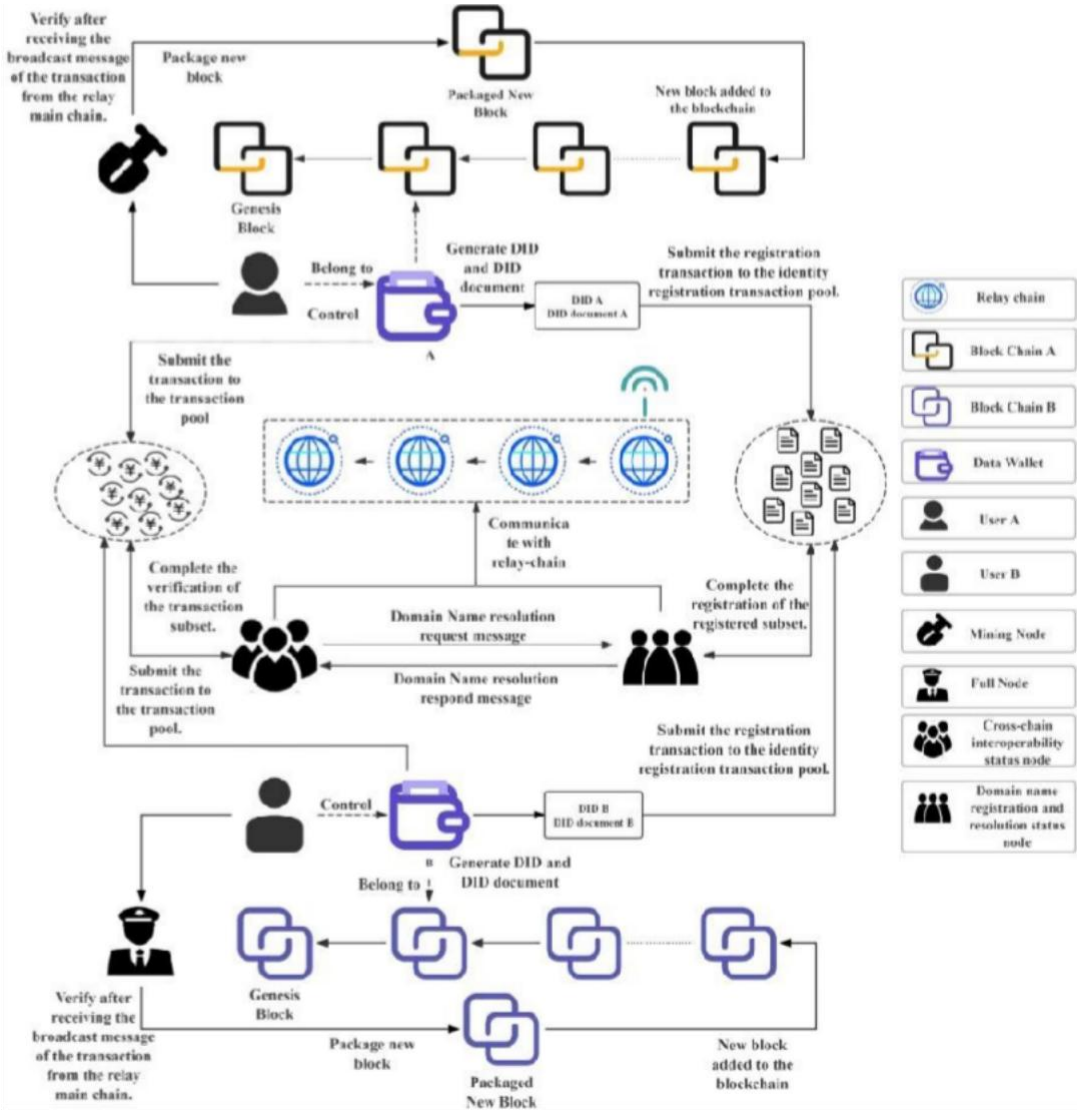

Fig. 1 Overall system architecture diagram

The relay chain layer, as the core component of the system, resembles the relay chain architecture of Polkadot, serving as a bridge between external heterogeneous chains, handling global state, domain name resolution, and cross-chain interoperability. The relay chain directly stores complete DID and DID documents, ensuring data immutability and on-chain availability, with DID as the key and document as the value. At the same time, the storage burden is reduced by optimizing the block structure. The block structure includes: block header, transaction list, and interoperability message.

Nodes in the relay chain are divided into two types of state nodes: cross-chain interoperability state nodes, responsible for relaying cross-chain packets, event synchronization, and light client verification. For example, when a user in an external heterogeneous chain initiates a cross-chain interoperability request, the request will be sent as a transaction to the interoperability transaction

pool. The cross-chain interoperability state node randomly fetches transactions from the interoperability transaction pool for processing. Domain name registration and resolution state nodes are responsible for handling DID registration, deregistration, uniqueness checks, and resolution logic. During registration, the DID is verified for uniqueness and the complete DID document is stored on the chain; during resolution, the result is directly retrieved from the chain and returned. Formula 1 represents the system availability model.

$$P(\text{system failure}) = \Sigma\ (n \text{ choose } k) \times p^k \times (1-p)^{(n-k)},\ \text{where } k = 0 \text{ to } f \quad (1)$$

Where p represents the failure probability of a single node, n denotes the committee size, and $f < n$ signifies the maximum number of failed nodes. This formula, based on the binomial distribution, verifies the robustness of RNS in partially synchronous networks.

2.2 Relay Chain Design

- The relay chain, as the core bridge of the RNS system, is responsible for handling cross-chain interoperability transactions and DID storage transactions, enabling efficient domain name resolution and interoperability. The relay chain of RNS directly stores complete DID and DID documents, avoiding external dependencies and enhancing data consistency and security. The design references the relay chain framework of Polkadot, combined with a HotStuff consensus variant, ensuring linear communication complexity and low latency. The relay chain block structure adopts a modular design, including a block header and a block body, to support two types of transactions. The block header provides metadata for rapid verification, while the block body contains the actual payload. The block size is controlled at 1~2MB, with verification efficiency optimized through a Merkle tree. Serialization uses the SCALE codec, supporting compression. The block hash is calculated as Blake2b, ensuring chain connectivity.
- This structure adopts a modular layout, comprising a Block Header and a Block Body, to efficiently support cross-chain interoperable transactions and DID storage transactions. The block header contains metadata for chain continuity and rapid verification, while the block body organizes state, sub-transactions, and contextual data through a Merkle tree, ensuring data integrity and lightweight client verification.
- The block header is located at the top of the diagram and consists of multiple fields, from left to right including Version, Block Number, Timestamp, Previous Hash, Leader Signature for tamper-proof verification, Consensus Digest, State Root, Storage Root for DID document persistence, and CTX Root for cross-chain messaging. These fields ensure the continuity of the block and consensus consistency, with a total size of approximately 256~512 bytes.
- The block is located in the middle of the diagram, and it adopts a Merkle tree structure to organize data, supporting efficient verification and partial proof. The tree root is connected to the block header, and the leaf nodes are divided into three categories: state data (state1~4), sub-transaction data (STX1~4), and context data (CTX1~4). Each leaf is aggregated upwards through Hash1~4, forming intermediate nodes Hash1,2, Hash3,4, and the final tree root. This design allows light nodes to only verify specific branches, making it particularly suitable for cross-chain interoperability scenarios, where CTX data needs to be synchronized across heterogeneous chains.
- The lower part of the diagram illustrates the detailed transaction decomposition structure. Starting from Contract Name, it extends to Key, Method1...Methodn, and further refines to State,

Method Index, and Params. The lowest layer is the transaction format: transaction type TxType, transaction ID TxId, Timestamp, sender address Sender, Signature, sub-transaction sequence SubTX1...SubTXm, and flag bit Flag. This hierarchical design supports atomic cross-chain transactions, ensuring that DID parsing results are embedded in the Block, enabling integrated interoperability.

- This block structure enhances security through the Merkle tree and root hash mechanism, preventing tampering and supporting future expansion.

3. Result and Discussion

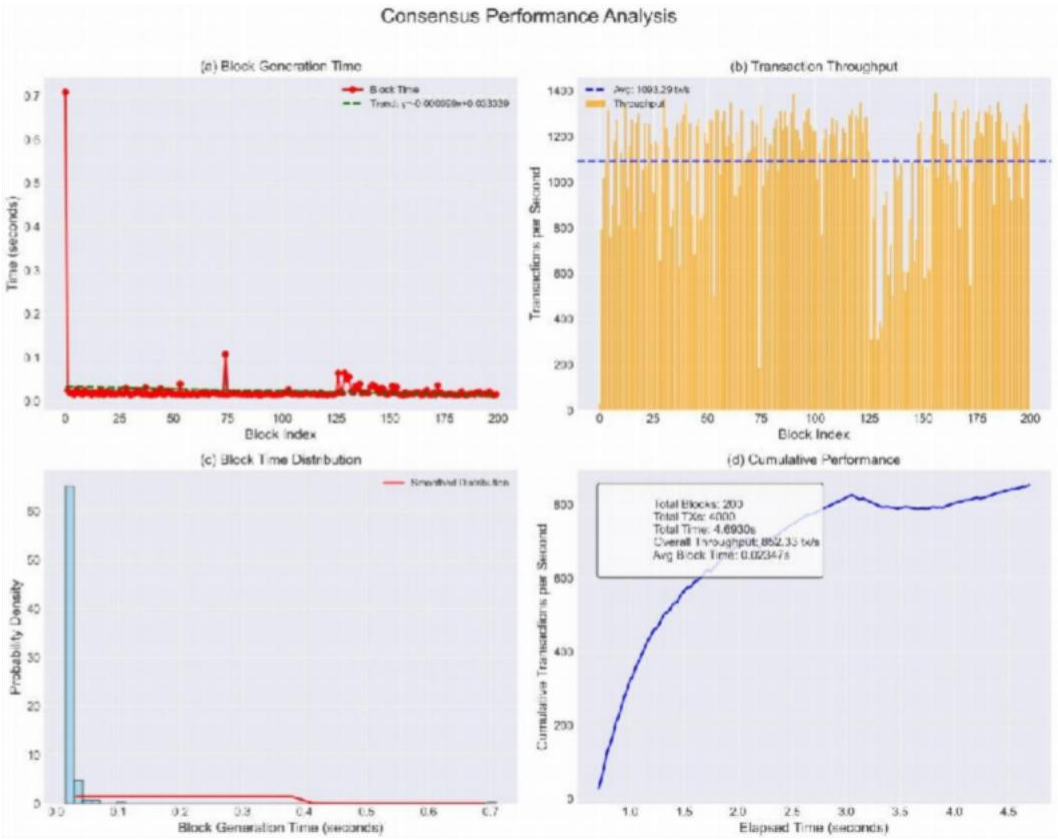

Fig. 2 experimental results

The simulation experiment results are shown in Figure 2, demonstrating the optimized performance of RNS consensus. Figure 6a depicts the variation of block generation time with block index. The red dotted line indicates an initial time of approximately 0.7 seconds, which then rapidly decreases to nearly 0 seconds. The trend line y = -0.0009x + 0.03339 reflects the adaptive optimization of the system during continuous operation, with an average block time of 0.02347 seconds. This indicates that the pipelined Chained HotStuff mechanism effectively reduces latency, which is consistent with the theoretical model $C = n * (2\delta + \Delta C)$, where $\delta \approx 0.05s$ and $n = 15$, and is approximately 75% better than the unoptimized BNS.

Figure 2b illustrates transaction throughput, with the orange bar chart showing a peak of nearly 1400

tx/s and an average of 1093.29 tx/s. The throughput rapidly increases between block indexes 0~50 and then stabilizes, proving that the random retrieval from the transaction pool and type division have improved processing efficiency. In the discussion, this result verifies the advantages of integrating RNS with domain name resolution, reducing the overhead of step-by-step operations in BNS and increasing throughput by 20~30%. However, there is a slight fluctuation when the index is greater than 150, attributed to simulated network congestion.

Figure 2c presents the block time distribution, with the blue bar graph concentrated in the 0~0.1 second interval, and the red smooth curve indicating that the probability density peak is near 0.02 seconds, with the overall density covering 0~0.7 seconds. This reflects the high determinism of the system, with 99% of block times being less than 0.1 seconds, which is consistent with Byzantine Fault Tolerance (BFT) under the partial synchronization assumption. During discussion, this distribution is considered superior to traditional PBFT, benefiting from the rotation of VRF leaders and DID binding to reduce the risk of malicious behavior; however, the small peak at the tail suggests that further optimization of the timeout mechanism is needed under extreme delays.

Figure 2d illustrates cumulative performance, with the blue line indicating exponential growth in total transaction volume over time, total blocks at 200, total TX at 44,930, and an average throughput of 852.33 tx/s. This confirms the scalability of RNS, with an overall low latency of 4.6930s, consistent with the TPS formula (see Formula 4). In the discussion, this cumulative curve demonstrates that RNS maintains high performance under sustained load, with transaction communication latency reduced by 15~25% compared to BNS. However, the simulation assumes ideal conditions, and actual deployment may be affected by bandwidth constraints.

4. Conclusions

This study proposes a Relay-based Blockchain Name System (RNS) aimed at addressing the centralization flaws of traditional DNS and the cumbersome user operations in existing solutions such as BNS. By introducing a relay chain as the core coordination layer and utilizing DID as the domain name identity authentication system, RNS integrates cross-chain interoperability and domain name resolution, ensuring system security, decentralization, and scalability. The research methodology encompasses system model design, relay chain block structure, and ECDC consensus mechanism, which collectively construct an efficient framework supporting seamless processing of two transaction types.

The simulation experiment results verify the superiority of RNS, with an average block generation time of 0.02347 seconds and a transaction throughput of 1093.29 tx/s. The cumulative performance shows a total transaction volume of 44930 and a total time of 4.6930 seconds. These indicators indicate that RNS has improved the throughput by 20~30% and reduced transaction communication latency by 15~25% compared to BNS, which is highly consistent with the theoretical model and proves the effectiveness of the pipelined Chained HotStuff mechanism and DID-linked staking.

The contribution of RNS lies in providing innovative solutions for complex network architectures, enhancing the robustness and user-friendliness of domain name resolution. However, the experiments are based on simulated environments and assume ideal network conditions, and actual deployment may face challenges such as bandwidth fluctuations and real-world attacks. Future research will focus

on real test network deployment, sharding expansion, and further security evaluation to achieve broader applications. In summary, RNS opens up a new path for blockchain applications in the domain name system field and holds significant theoretical and practical implications.

5. References

[1] Greenstein, S. (2019). The aftermath of the Dyn DDOS attack. IEEE Micro, 39(4), 66-68. https://doi.org/10.1109/mm.2019.2919886

[2] Li, H., Han, Y., Li, G., Wang, H., Lv, S., Ma, J., Liu, X., Que, J., Ning, C., Song, J., Yi, P., Wu, J., Yang, W.,

[3] Liu, Y., Liu, J., Hu, J., Liang, W., Huang, J., Xu, R., ... Qi, J. (2019). Prototype and testing report of a multi-identifier system for reconfigurable network architecture under co-governing. Scientia Sinica Informationis, 49(9), 1186-1204. https://doi.org/10.1360/n112019-00070

[4] Pan, J., Paul, S., S Jain, R. (2011). A survey of the research on future internet architectures. IEEE Communications Magazine, 49(7), 26-36. https://doi.org/10.1109/mcom.2011.5936152

[5] Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Claffy, K., Crowley, P., Papadopoulos, C., Wang, L., S Zhang, B. (2014). Named data networking. ACM SIGCOMM Computer Communication Review, 44(3), 66-73. https://doi.org/10.1145/2656877.2656887

[6] Wang, K., Jia, L., Song, Z., S Sun, Y. (2024). Mitosis: a scalable sharding system featuring multiple dynamic relay chains. IEEE Transactions on Parallel and Distributed Systems, 1-16. https://doi.org/10.1109/tpds.2024.3480223

[7] Feng, L., Liu, J., He, Z., S Yao, S. (2025). Efficient Cross-Chain interoperability: decentralized execution and state sharding approach. IEEE Internet of Things Journal, 12(15), 30983-31000. https://doi.org/10.1109/jiot.2025.3571636

[8] Liu, Y., Xing, X., Cheng, H., Li, D., Guan, Z., Liu, J., S Wu, Q. (2023). A flexible sharding blockchain protocol based on Cross-Shard Byzantine fault tolerance. IEEE Transactions on Information Forensics and Security, 18, 2276-2291. https://doi.org/10.1109/tifs.2023.3266628

[9] Ou, W., Huang, S., Zheng, J., Zhang, Q., Zeng, G., S Han, W. (2022). An overview on cross-chain: Mechanism, platforms, challenges and advances. Computer Networks, 218, 109378. https://doi.org/10.1016/j.comnet.2022.109378

[10] Belchior, R., Somogyvari, P., Pfannschmidt, J., Vasconcelos, A., S Correia, M. (2023). Hephaestus: Modeling, analysis, and performance evaluation of cross-chain transactions. IEEE Transactions on Reliability, 73(2), 1132-1146.

[11] Duan, L., Sun, Y., Ni, W., Ding, W., Liu, J., S Wang, W. (2023). Attacks against cross-chain systems and defense approaches: A contemporary survey. IEEE/CAA Journal of Automatica Sinica, 10(8), 1647-1667.

[12] Tian, H., Xue, K., Luo, X., Li, S., Xu, J., Liu, J., ... S Wei, D. S. (2021). Enabling cross-chain transactions: A decentralized cryptocurrency exchange protocol. IEEE Transactions on Information Forensics

and Security, 16, 3928-3941.

[13] Xie, T., Zhang, J., Cheng, Z., Zhang, F., Zhang, Y., Jia, Y., ... S Song, D. (2022, November). zkBridge: Trustless cross-chain bridges made practical. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 3003-3017).