American Academic Scientific Research Journal for Engineering, Technology, and Sciences
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402
https://asrjetsjournal.org/index.php/American_Scientific_Journal/index

# Cross-Blockchain Interoperability Mechanisms: Bridges, Light Clients and Relayer Protocols

Yevhenii Shcherbina*

*Software Engineer, Coder Inc,Boston, Massachusetts, USA*
*Email:evgeniy.shcherbina.es@gmail.com*

**Abstract**

The article is devoted to the study and comparative analysis of mechanisms for enabling cross-chain interaction, including bridges, light clients, and relayer-based protocols. The relevance of the work is determined by the growing fragmentation of the blockchain ecosystem, where isolated networks cannot efficiently exchange data and assets, which restrains their widespread adoption. The novelty lies in a comprehensive approach to the classification and evaluation of existing solutions according to criteria such as security, decentralization, and efficiency. Within the work, the fundamental problems of interoperability and the architectural principles of various mechanisms are described. Centralized and decentralized bridges, protocols based on light clients (for example, IBC), and relayer networks are examined. Special attention is paid to the analysis of their trust models and attack vectors. The study aims to conduct a comparative analysis of these approaches to identify their strengths and weaknesses. To achieve this goal, methods of systematic analysis of the scientific literature, comparative analysis, and synthesis are used.The article will be useful for developers of blockchain systems, researchers, and architects of decentralized applications working on the creation of integrated and scalable solutions.

***Keywords:*** interoperability; cross-chain; blockchain bridges; light clients; relay protocol; IBC; decentralization; blockchain security; atomic swap; sidechains.

---

*Received: 8/30/2025*
*Accepted: 10/30/2025*
*Published: 11/8/2025*

---

* *Corresponding author.*

## 1.Introduction

Since the advent of Bitcoin, the distributed ledger ecosystem has expanded into thousands of autonomous and technologically heterogeneous networks. Each of them—be it Ethereum, Solana, or Polkadot—functions as a separate digital jurisdiction with its own consensus rules, transaction format, and smart contract computation model. Such fragmentation creates substantial barriers: assets cannot be freely transferred across domains, and decentralized applications (dApps) remain confined within individual ecosystems. The absence of native, cryptographically grounded inter-network communication remains one of the principal obstacles to achieving Web3 as a coherent network of networks. Removing this barrier will unlock opportunities for sophisticated cross-chain applications, enhance asset liquidity, and increase the practical value of the technology [8].

**The aim** of this work is to conduct a comprehensive comparative analysis of modern inter-network interaction mechanisms, identifying their strengths, limitations, and inherent trade-offs across the dimensions of security, decentralization, and efficiency.

To achieve this aim, the following tasks are proposed:

— systematize and describe the key approaches to interoperability: cross-chain bridges (centralized and decentralized), as well as protocols based on light clients and networks of relayers;

— perform a comparative analysis of the specified mechanisms along basic parameters: trust model, level and type of security, scalability, latency, and implementation/operational complexity.

**The scientific novelty** lies in integrating disparate information about particular interoperability technologies into a unified comparative framework that explicitly articulates the fundamental trade-offs between trust and performance. Unlike works that focus on a single class of solutions, the proposed approach offers a holistic, end-to-end perspective on the problem.

**The author's hypothesis** is that protocols minimizing reliance on intermediaries—primarily constructions based on light clients and relayers (for example, IBC)—constitute a more resilient and secure paradigm for the long-term development of interoperability compared to systems that depend on trusted federations of validators, despite their increased implementation complexity.

The limitations of this study are its theoretical and systematic nature; it does not include quantitative performance benchmarks, formal security verification of the analyzed protocols, or an empirical analysis of the economic attack vectors and incentive models for relayers and validators.

## 2.Materials and methods

To write the article, the method of systemic analysis of the scientific literature was applied to form the theoretical basis of the study. The comparative method was used to juxtapose different interoperability mechanisms according to selected criteria (trust model, security, scalability). The synthesis method was applied to generalize the obtained

data and to formulate conclusions regarding the prospects of particular approaches.The semantic blocks are as follows: taxonomic and methodological surveys: Belchior R., Vasconcelos A., Guerreiro S., Correia M. [1]; Ren K., Ho N. M., Loghin D., Nguyen T. T., Ooi B. C., Ta Q. T., Zhu F. [2]; Han P., Yan Z., Ding W., Fei S., Wan Z. [3]; early survey Qasse I. A., Abu Talib M., Nasir Q. [5]; specification and industrial standard of light-client verification — Interchain Foundation (IBC) [4]; security of cross-chain bridges: Augusto A., Belchior R., Correia M., Vasconcelos A., Zhang L., Hardjono T. [7]; Zhang M., Zhang X., Zhang Y., Lin Z.[9]; channel/HTLC approaches: Poon J., Dryja T. [8]; engineering integration patterns and practices: Shcherbina Y., Mesyura V. Reference [10]; applied perspective of the healthcare domain: Reegu F., Daud S. M., Alam S. [6].The surveys establish a single classification axis by trust and verification models: from on-chain verification of a foreign state via light clients/cryptographic proofs to bridges with external validators and HTLC-based atomic swaps. Belchior R., Vasconcelos A., Guerreiro S., Correia M. [1] introduces the triad engines/connectors/cryptocurrency-oriented approaches. Ren K., Ho N. M., Loghin D., Nguyen T. T., Ooi B. C., Ta Q. T., Zhu F. [2] clarifies stack layers and types of verification (native, external, conditional, provable). Han P., Yan Z., Ding W., Fei S., Wan Z. [3] frames engineering trade-offs between security and performance. IBC from the Interchain Foundation [4] institutionalizes the TAO model (transport–authentication–ordering): each chain maintains a light client of its counterparty, the relayer is not privileged, and proof verification occurs on the receiving chain; the ICS specifications (including ICS-20) normalize packet semantics and the handshakes of connections/channels. The survey by Qasse I. A., Abu Talib M., Nasir Q. [5] records the pre-reference stage of the field, where heterogeneous bridges without a standard and notary schemes dominated. This fundamental block of work is crucial because it provides a taxonomic framework for the paper. The consensus between these studies is that compatibility is a range of trust models, from internal verification to external notaries, which directly affects the comparative criteria of this study. They prove that there is no "universal" solution, which confirms the purpose of this article - to analyze the specific trade-offs inherent in each model.

Bridge security is the central motif of recent years. Augusto A., Belchior R., Correia M., Vasconcelos A., Zhang L., Hardjono T. [7] systematize threats according to the paradigms trusted notary/multisig, optimistic bridges with a dispute period, validating/ZK bridges, emphasizing formal security and privacy invariants. Zhang M., Zhang X., Zhang Y., Lin Z. [9] detail the attack surface (key compromise, logic errors of lock-mint/burn-unlock, finality mismatches, data removal/DA risks) and map countermeasures: protocol limiting, multi-level event verification, distributed keys/rotation, transition to on-chain verification of proofs. Poon J., Dryja T. [8] show how HTLC and a network of payment channels provide cross-chain atomic exchanges with a minimal trust surface, at the price of requirements for script/timelock compatibility and the presence of watchers. Practice-level engineering articles, such as the work of Shcherbina Y., Mesyura V.[10], describe lock-mint/burn-unlock patterns and their operational constraints. In the applied healthcare domain, Reegu F., Daud S. M., Alam S. [6] finds that interoperability is often reduced to compatibility of data standards (EHR/HL7/FHIR), access policies, and regulatory compliance; permissioned networks and trusted gateways are used here more often than fully crypto-provable bridges. These articles confirm that the vast majority of financial losses occur in federated bridge models, precisely where a set of external validators is trusted. This strongly supports the author's hypothesis and highlights the urgent need to move towards models that rely on on-chain verification rather than operational multi-signal security.

In sum, the contours of approaches are as follows. The standardized light-client branch (IBC) seeks to transfer the security guarantee to the receiving L1, reducing the role of the relayer to transport [1-5] converge on the view that the- degree of trustless is determined by which chain verifies the foreign state and what assumptions are made about finality/DA. The paradigm bridge as a quorum of external validators remains engineeringly straightforward but is vulnerable to operational/key risks [7, 9]; the HTLC/channel branch [8] minimizes trust but is limited by expressiveness and UX. The applied requirements of industries [6] often demand not state-to-state bridges but reliable data semantics and access control.

However, there are contradictions in the research:

1. The term trustless: part of the works applies it even to external multisigs, whereas the surveys and IBC in fact tie trustless to on-chain verification of a foreign consensus/execution [1, 2, 4].
2. Different protection priorities: SoK works emphasize formal invariants and privacy [7], whereas the RAID review records the dominance of exploits of the operational layer and key infrastructure [9].
3. Finality: part of the literature implicitly proceeds from deterministic BFT finality (IBC compatibility), whereas for probabilistic/deferred finality the security conditions and timings become more complex [8, 9]. Weakly covered are: economic robustness of bridges given TVL and attack costs; liveness under prolonged asynchrony and reorg robustness; incentives/slashing for relayers and the problem of censorship and cross-chain MEV; the life cycle of client/proof updates (ICS migrations, key rotation); privacy of cross-chain calls and compatibility with ZK; mechanically checkable specifications of invariants and their deployment in production code.

**3.Results**

Each blockchain constitutes a closed system of state verification. The consensus achieved within a network (for example, Bitcoin) has no authority or awareness of events in another network (for example, Ethereum). This mutual blindness is a fundamental barrier. To transfer an asset or information from chain A to chain B, a mechanism is required that can:

- Reliably attest to an event in chain A (for example, the locking of tokens).

- Securely deliver this attestation to chain B.

- Ensure the corresponding action in chain B (for example, the issuance of wrapped tokens).

All existing solutions address this triad of tasks in one way or another, but with different trust and security models. Bridges are the most common yet the most heterogeneous class of solutions. They can be divided into two broad groups: centralized (trusted) and decentralized (trustless or trust-minimized).

Centralized (trusted) bridges. These systems rely on one or several trusted intermediaries (a federation) that control the asset transfer process. The canonical workflow is as follows: a user sends an asset to an address controlled by the federation in chain A; the federation confirms receipt and issues an equivalent asset in chain B

from its address.Decentralized bridges (validator-based). These bridges aim to mitigate centralization risks by employing a set of independent validators that monitor events in both chains and collectively sign transactions for the issuance/unlocking of assets. Examples include Wormhole and Multichain (prior to the incident) [1, 3].

Protocols based on light clients are also of interest. This approach is among the most secure and decentralized. Instead of trusting intermediaries, a smart contract in one chain (chain B) verifies the state of another chain (chain A) directly. This is achieved by implementing a light client of chain A as a smart contract in chain B. The light client tracks the block headers of chain A, enabling it to verify the authenticity of transactions and events in chain A using cryptographic proofs (Merkle proofs) without the need to trust any party.

Cosmos Inter-Blockchain Communication (IBC). IBC is the gold standard for this approach. Each chain in the Cosmos ecosystem runs a light client of the other chains with which it interacts.

There are also relayer- and oracle-based protocols. This approach represents a compromise between trusted bridges and heavyweight light clients. It employs a network of external actors (relayers or oracles) that do not validate transactions but only transmit signed data and proofs from one chain to another. Data authenticity is checked by on-chain contracts, but without the full logic of a light client. Examples include LayerZero and certain sidechain implementations [2, 7].

Table 1 will present a comparative analysis of different approaches to ensuring security in blockchain systems.

**Table 1:** Comparative analysis of different approaches to ensuring security in blockchain systems [1, 2, 3, 7]

| Criterion | Centralized bridges | Decentralized bridges (validators) | Light clients (IBC) | Relayers (LayerZero) |
|---|---|---|---|---|
| Trust model | Trust in the operator | Trust in M of N validators | Trustless (trust in the networks' consensus) | Trust in the independence of the oracle/relayer |
| Security | Low (single point of failure) | Medium (risk of collusion) | Very high | Medium-high |
| Decentralization | Low | Medium | High | Medium |
| Cost | Low | Medium | Very high | Low-medium |
| Latency | Low | Low-medium | High | Low-medium |
| Complexity | Low | Medium | Very high | Medium |

Thus, it can be observed that there is no universal solution for cross-chain interaction. The choice of mechanism is always a trade-off, primarily between security/decentralization and cost/complexity. Centralized bridges, despite their vulnerabilities, remain popular due to their ease of use and low transaction costs. Light client-based protocols, such as IBC, offer a golden standard of security, but their deployment beyond homogeneous ecosystems

(such as Cosmos) remains an extremely challenging task. This leads to the notion that the future of interoperability lies not in the dominance of a single approach, but in their hybridization and specialization.

**4.Discussion**

The comparative analysis presented in the Results section (Table 1) clearly illustrates the fundamental trilogy of interoperability: the system cannot be optimized simultaneously in terms of security, decentralization, and low cost/complexity. The results show that the Light Client (IBC) protocols represent the basis of security, since they "trust the consensus of networks" [4]. However, their high cost and complexity make them impractical for many heterogeneous interactions (e.g. EVM-with-non-EVM). Conversely, centralized and validator-based bridges dominate in terms of cost and speed, but pose significant systemic risk, as evidenced by the security literature reference [7, 9]. This compromise is not a temporary technical obstacle, but a permanent architectural limitation. The industry's reliance on "medium-sized" security verification bridges is a pragmatic compromise that has led to billions in losses, confirming the relevance of a more sustainable paradigm.

This analysis directly confirms the author's hypothesis that protocols based on minimizing trust are more stable, but at the same time highlights their practical limitations. Thus, the discussion should go beyond simply stating that IBC is the best, and consider how to apply this security system in a fragmented and cost-sensitive ecosystem. It is for this reason that the Adaptive Hybrid Interoperability Architecture (AHIA) was proposed (Fig. 1).

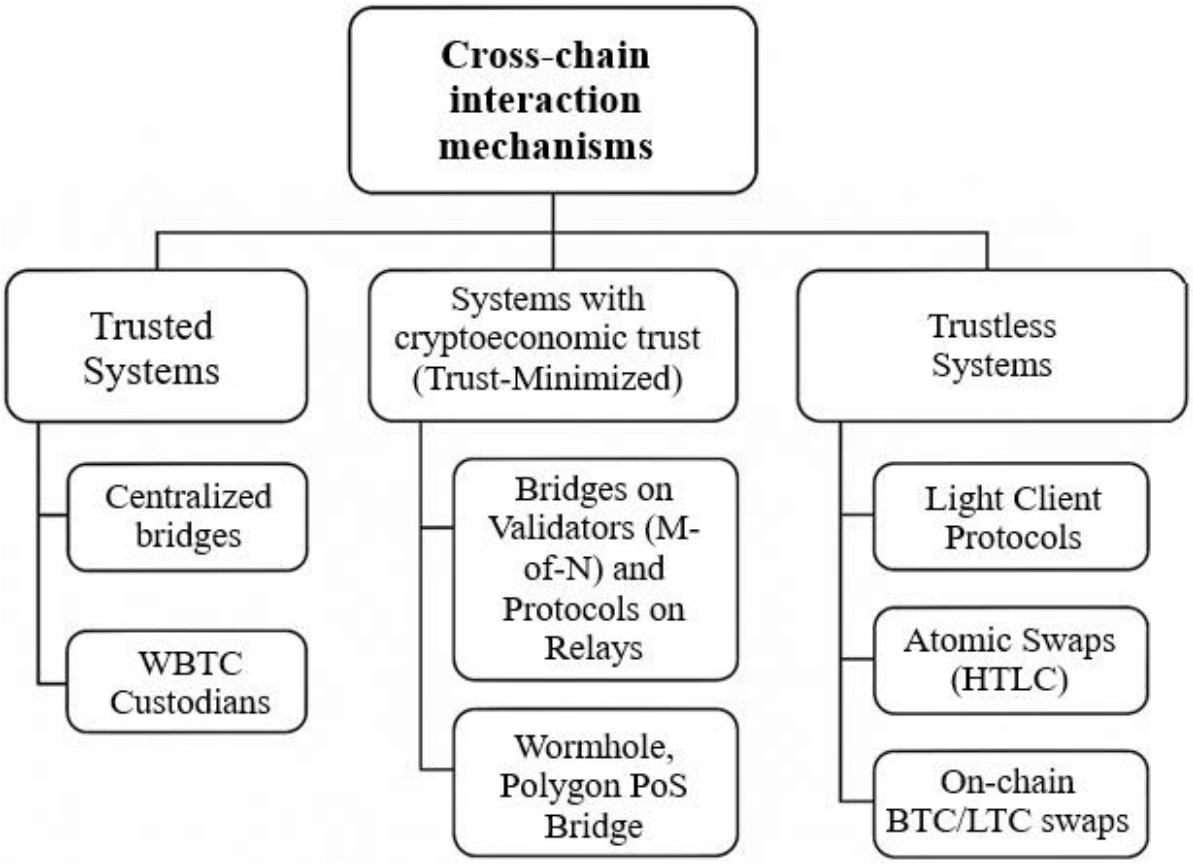


**Figure 1:** Taxonomy of cross-chain interaction mechanisms based on the trust model [2, 4, 5]

The idea of AHIA is not to create a single bridge for all, but to build a multi-layered system in which the choice of the data/asset transfer mechanism depends on the context of the transaction: its value, speed requirements, and security criticality (Fig. 2).

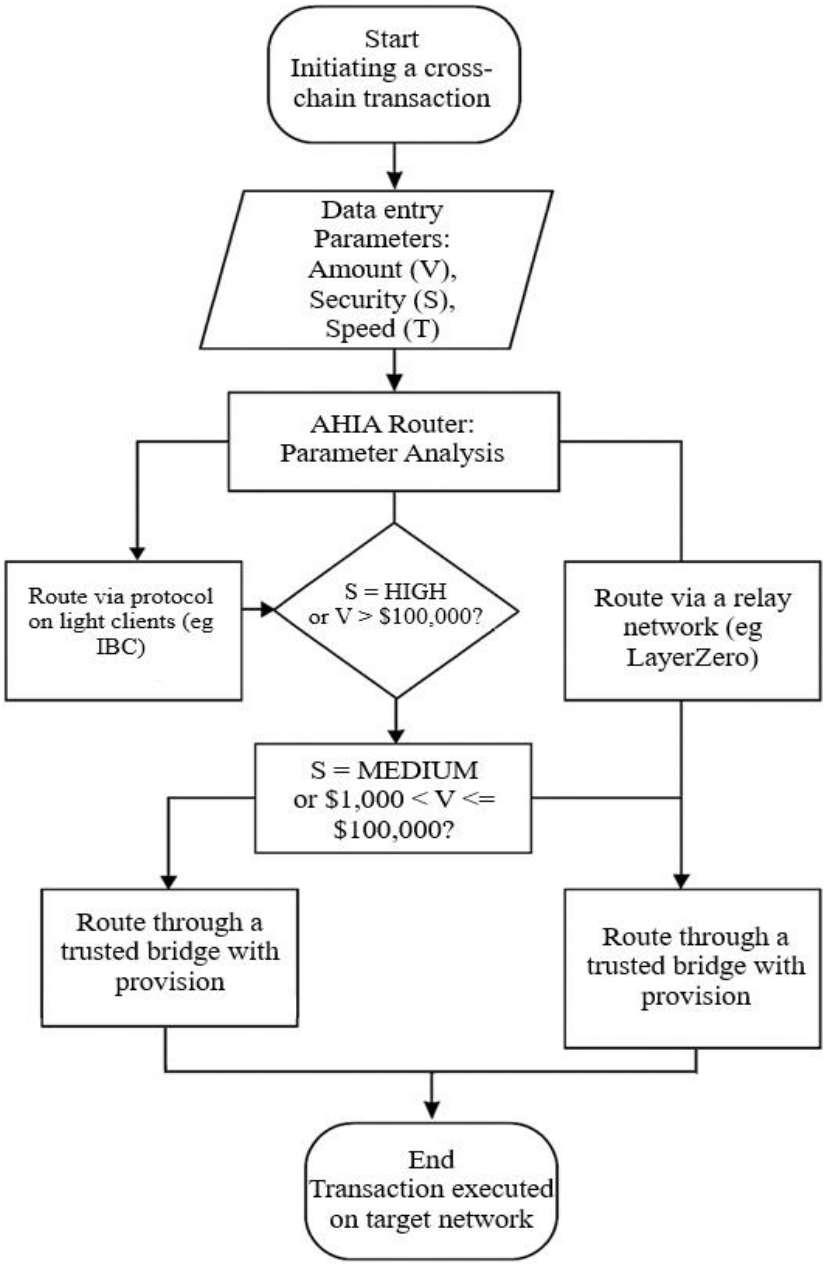


**Figure 2:** The scheme of the Adaptive Hybrid Architecture (AHIA) [6, 7]

Within this architecture, applications can adaptively select the transport layer that matches their value-at-risk, latency tolerance, and trust assumptions. A retail-sized transfer—say, $10 in USDC—can rationally traverse a fast, inexpensive custodial bridge whose residual risk is acceptable at that scale. By contrast, cross-chain DAO governance, where proposals may steer assets worth millions, should be confined to slow, costlier pathways that maximize security via light-client verification and strong on-chain finality. This stratification echoes scaling doctrine: not every transaction needs the same security budget, a point underscored by research on Layer-2

systems.The linchpin of AHIA is a router—a smart contract or protocol that computes and enforces an optimal route subject to user and application constraints. Functionally, this router aggregates and arbitrages liquidity across heterogeneous bridges and interoperability protocols, returning end-to-end quotes that reflect not only price and latency but also the implied trust model and security level [9, 10].

Accordingly, the industry should pivot from seeking a one-size-fits-all "holy grail" to standardizing interfaces and building aggregator layers that let applications flexibly compose the best tool for each job. The proposed hybrid architecture AHIA provides a conceptual and practical scaffold for such systems, raising the resilience and operational efficiency of the cross-chain ecosystem—fully consistent with the broader shift from monolithic designs toward modular, specialized blockchain stacks.

## 5.Conclusion

The study met its central objective: it delivered a rigorous, side-by-side appraisal of the dominant approaches to cross-chain interoperability. Specifically, it dissected three architectural paradigms— bridge designs anchored in centralized custody or validator committees, light-client protocols exemplified by IBC, and relayer-orchestrated schemes—and showed that their decisive point of divergence is the underlying trust assumption, ranging from reliance on an off-chain custodian or committee to on-chain, cryptographic verification of foreign state.

Evaluated against security, decentralization, cost, and implementation/operational complexity, the trade-offs are unambiguous. Light-client designs offer the strongest security guarantees and the most trust-minimized posture, but they impose the heaviest burden in engineering effort and on-chain verification costs. At the opposite extreme, centralized bridges deliver low latency and low fees by substituting security with institutional trust, thereby concentrating control and increasing custodial/key-management risk. Relayer networks occupy a middle ground: they mitigate some custodial exposure and can be more cost-efficient than full light-client verification, yet they inherit coordination risks, routing/liveness concerns, and residual trust in external actors. In short, no paradigm dominates across all criteria; selecting an approach entails an explicit choice of trust model and a principled acceptance of its attendant cost and complexity profile.

The vulnerability analysis confirmed the author's hypothesis that protocols with minimization of trust (trustless) are the most resilient in the long term. However, their direct implementation is not always practical. As a promising direction, the Adaptive Hybrid Interoperability Architecture (AHIA) was proposed, which does not seek a single solution but offers a framework for the dynamic selection of the optimal mechanism depending on the transaction context.

The final conclusion is that the future of cross-chain interaction lies with modular and hybrid systems that can provide developers and users with a flexible toolkit, rather than with a monolithic bridge for all. This approach makes it possible to combine the advantages of different models, minimizing their drawbacks and increasing the overall reliability and efficiency of the global blockchain ecosystem.

**References**


[1]. Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. Acm Computing Surveys (CSUR), 54(8), 1-41. https://doi.org/10.1145/347114

[2]. Ren, K., Ho, N. M., Loghin, D., Nguyen, T. T., Ooi, B. C., Ta, Q. T., & Zhu, F. (2023). Interoperability in blockchain: A survey. IEEE Transactions on Knowledge and Data Engineering, 35(12), 12750-12769. https://doi.org/10.1109/TKDE.2023.3275220 .

[3]. Han, P., Yan, Z., Ding, W., Fei, S., & Wan, Z. (2023). A survey on cross-chain technologies. Distributed ledger technologies: research and practice, 2(2), 1-30. https://doi.org/10.1145/3573896.

[4]. Interchain Foundation. (2023). Inter-Blockchain Communication Protocol (IBC). IBC Protocol. Retrieved from https://ibcprotocol.org/ (date of access: 25.07.2025)

[5]. Qasse, I. A., Abu Talib, M., & Nasir, Q. (2019, March). Inter blockchain communication: A survey. In Proceedings of the ArabWIC 6th Annual International Conference Research Track (pp. 1-6). https://doi.org/10.1145/3333165.3333167.

[6]. Reegu, F., Daud, S. M., & Alam, S. (2021). Interoperability Challenges in Healthcare Blockchain System-A Systematic. Annals of RSCB, 25(4), 15487-15499.

[7]. Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L., & Hardjono, T. (2024, May). Sok: Security and privacy of blockchain interoperability. In 2024 IEEE Symposium on Security and Privacy (SP) (pp. 3840-3865). IEEE. https://doi.org/10.1109/SP54263.2024.00255.

[8]. Poon, J., & Dryja, T. (2016, January). The bitcoin lightning network: Scalable off-chain instant payments.

[9]. Zhang, M., Zhang, X., Zhang, Y., & Lin, Z. (2024, September). Security of cross-chain bridges: Attack surfaces, defenses, and open problems. In Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses (pp. 298-316). https://doi.org/10.1145/3678890.3678894.

[10]. Shcherbina, Y., & Mesyura, V. (2021). Mechanisms for integrating blockchains with each other. Visnyk of Vinnytsia Politechnical Institute, (2), 85-91.