Universal Library of Innovative Research and Studies Research Article

ISSN: 3065-0003 | Volume 2, Issue 3

Open Access | PP: 49-53

DOI: https://doi.org/10.70315/uloap.ulirs.2025.0203008

Lightning Network Protocol Architecture and its Role in Blockchain Scalability

Yevhenii Shcherbina

Software Engineer, Coder Inc, Boston, Massachusetts, USA.

Abstract

The article is devoted to the analysis of the Lightning Network protocol architecture and its role in addressing the blockchain scalability problem. The relevance of the study is driven by the growing throughput requirements of decentralized networks that cannot be met at the base layer (Layer-1). The novelty lies in the systematization and analysis of recent research on economic models, security, and network topology. The work describes the fundamental scalability limitations of blockchains using Bitcoin as an example and examines the key components of the Lightning Network: payment channels and hashed timelock contracts (HTLC). Special attention is paid to payment routing mechanisms and liquidity management challenges. The study sets the objective of assessing the effectiveness and maturity of the protocol as a second-layer solution. To achieve this objective, methods of systematic literature review and comparative analysis are employed. The conclusion outlines the advantages of the protocol, as well as unresolved issues such as the risk of centralization and routing complexity. The article will be useful for researchers, developers, and specialists in the field of blockchain technologies.

Keywords: *Lightning Network, Blockchain, Scalability, Bitcoin, Layer-2, Payment Channels, HTLC, Micropayments, Payment Routing, Decentralization.*

INTRODUCTION

Blockchain – originally instantiated in Bitcoin – introduced a cryptographically verifiable, append-only ledger that dispenses with a central gatekeeper while hardening against unauthorized state changes. Yet the surge in real-world usage exposed architectural bottlenecks. Foremost is throughput: canonical Layer-1 designs such as Bitcoin process only a handful of transactions per second, orders of magnitude below the capacity required for global retail payments. This tension is commonly framed as the "trilemma," i.e., the structural difficulty of optimizing scalability, security, and decentralization at once. In response, research and engineering have pivoted toward Layer-2 constructions. Among these, the Lightning Network (LN) has emerged as a comparatively mature approach for real-time, low-fee micropayments; a rigorous appraisal of its design choices and empirical performance is therefore consequential for the evolution of the broader blockchain stack [1, 6].

Aim of the study: To investigate the Lightning Network's architecture and to evaluate its capacity to mitigate blockchain-level scalability constraints in light of contemporary scientific evidence.

OBJECTIVES

- Diagnose the root causes of scalability limits in first-layer blockchains, using Bitcoin's consensus and data-propagation pipeline as the reference model.
- Explicate the Lightning Network's protocol architecture, detailing its core primitives–bidirectional payment channels, commitment transactions, and hashed timelock contracts (HTLC)–and how they compose into multi-hop payments.
- Assess LN's effectiveness as a scaling mechanism by weighing demonstrated advantages (latency reduction, fee minimization) against current challenges (path-finding and routing reliability, liquidity provisioning and rebalancing, security failure modes, and centralization pressures in network topology).

The scientific novelty of the study lies in the systematization and analysis of research devoted to the evolution of the LN protocol. Unlike early works that focused on the theoretical model, this study emphasizes empirical data on network topology, the economic incentives of participants, and new

Citation: Yevhenii Shcherbina, "Lightning Network Protocol Architecture and its Role in Blockchain Scalability", Universal Library of Innovative Research and Studies, 2025; 2(3): 49-53. DOI: https://doi.org/10.70315/uloap.ulirs.2025.0203008.

attack vectors, which makes it possible to form an up-to-date view of the state of the technology.

Regarding the **author's hypothesis**, it is assumed that although the Lightning Network increases the transactional throughput of the blockchain and makes micropayments economically viable, its long-term sustainability and decentralization critically depend on solving the problems of routing efficiency and liquidity management. Without new protocol improvements, the network may evolve toward a centralized hub-and-spoke topology, which contradicts the foundational principles of blockchain.

MATERIALS AND METHODS

A systematic analysis and synthesis of current scientific literature on the architecture and functioning of the Lightning Network protocol were conducted for this article. The corpus of works on the Lightning Network (LN) coalesces into six compact directions. Architecture and standardization are defined by the canonical model of bilateral channels with HTLC and penalty commitments, which moves settlement off L1 while preserving security (Poon J., Dryja T. [6]); operationalization is specified in the BOLTs – message formats, the gossip layer, Sphinx routing, and extensions such as MPP (Russell, R., et al. [10]), and a survey of the evolution records the shift toward liquidity providers and new business models and summarizes the engineering–economic trade-offs of scaling (Dasaklis T. K., Malamas V. [5]). The network-structural perspective shows how, from a sparse graph, percolation mechanisms form a giant component sensitive to channel opening costs and the distribution of limits (Bartolucci S., Caccioli F., Vivo P. [9]); empirical analysis of centralities on network snapshots reveals a core of nodes with high betweenness/degree and associated systemic risks (Zabka P., Förster K. T., Decker C., Schmid S. [7]), whereas the equilibrium theory of the LN economy rationalizes the stability of a core–periphery topology under positive fixed costs and stochastic payment flows (Guasoni P., Huberman G., Shikhelman C. [11]). The algorithmic–operational layer links scalability with liquidity management: the imbalance metric and proactive cycle-based rebalancing reduce failure probability and throughput degradation under asymmetric flows (Pickhardt R., Nowostawski M. [8]), and optimal route search adapts shortest paths to LN cost and reliability metrics with consideration of limits and success probability (Shcherbina Y., Mesyura V. [12]). Security and privacy reveal bottlenecks: due to the limited number of parallel HTLC slots, low-cost congestion/jamming attacks are possible that sharply reduce the share of successful payments (Mizrahi A., Zohar A. [3]), and correlation and active analyses, despite the onion scheme of Sphinx, deanonymize participant roles and partially disclose routes (Kappos G., Yousaf H., Piotrowska A., Kanjalkar S., Delgado-Segura S., Miller A., Meiklejohn S. [4]). The economic framework ties technical design to the monetary function of Bitcoin: reduced latency and fee predictability make LN suitable for everyday money, but the sustainability of router profitability remains dependent on volume and fee structure (Divakaruni A., Zimmerman P. [2]). Finally, a demonstration of a quantum SVM on the cryptanalysis of the Caesar cipher illustrates interest in quantum-ML approaches in the cryptographic analysis of protocols (Kim H. J., Song G. J., Jang K. B., Seo H. J. [1]).

Overall, the literature diverges along two lines: the drive for efficiency through routing centralization, theoretically and empirically substantiated [7, 11], conflicts with the goals of privacy and resilience in the presence of observers and jamming threats [3, 4]. Underexplored are: reproducible empirical evidence on the effectiveness of MPP/AMP and dynamic pricing on live topology, standardized and UX-preserving countermeasures to congestion in the BOLTs [10], the economics of liquidity markets and LSP pricing, as well as LN behavior under L1 fee shocks and prolonged outages.

The study also used prior works, in particular, by Shcherbina Y., Mesyura V. [12] where models for representing the Lightning Network and algorithms for finding optimal payment routes were previously investigated, which was taken into account in the analysis of routing mechanisms.

The following research methods were applied:

- Systematic analysis and synthesis of scientific literature to form a holistic understanding of the protocol.

- Structural analysis to decompose the Lightning Network architecture into key components.

- Comparative method to compare LN with first-layer solutions and other Layer-2 protocols.

RESULTS

To understand the significance of the Lightning Network, it is first necessary to consider the architectural constraints of the base blockchain layer, a vivid example of which is Bitcoin. A blockchain is a distributed ledger consisting of a sequential chain of blocks, each of which contains a set of transactions. New blocks are added to the chain by means of a consensus mechanism (in Bitcoin, Proof-of-Work) that requires participants (miners) to solve a computationally hard problem.

The scalability problem is embedded in two key protocol parameters:

1. Block size: In Bitcoin it is limited, which constrains the number of transactions that can be included in a single block.
2. Block creation time.

The product of these two parameters determines the maximum throughput of the network. A naive attempt simply to increase the block size would lead to network centralization, since only powerful nodes would be able to store and process the ever-growing blockchain, which undermines the technology's key advantage, decentralization [6].

The Lightning Network offers a solution to this problem by moving the bulk of transactions outside the main blockchain (off-chain). The idea is to use the blockchain not as a processing center for each individual transaction, but as a final arbitration layer for settlement.

LN is a network of bidirectional payment channels created between two participants. Within such a channel the parties can conduct an unlimited number of instantaneous transactions without recording each of them on the blockchain. Only two transactions require recording in the main ledger: the channel opening transaction and the channel closing transaction.

The architecture of LN is based on several key Bitcoin cryptographic and scripting primitives. Payment channels To open a channel, two participants (for example, Alice and Bob) create a special transaction, a Funding Transaction. They both contribute a certain amount of BTC that is locked at a 2-of-2 multisig address. This means that subsequent spending of these funds requires the signatures of both Alice and Bob. This transaction is recorded on the blockchain, fixing the channel opening and its initial capacity.

Commitment transactions: After the channel is opened, Alice and Bob can exchange funds. Each transfer of funds is, in essence, an update of the balance within the channel. This update occurs through the creation and exchange of commitment transactions. These are standard, but not broadcast to the network, Bitcoin transactions that spend funds from the multisig address and distribute them in accordance with the current balance [2, 6].

A problem arises: if Alice and Bob have executed 100 transactions, they will hold 100 versions of commitment transactions. What prevents Alice from broadcasting to the network an old version in which the balance was more favorable to her? This problem is solved by the mechanism of revocable sequence maturity contracts (RSMC). Each new commitment transaction renders the previous one invalid. If one of the parties attempts to cheat by broadcasting an old transaction, the injured party gains the opportunity to take all funds from the channel as a penalty. This creates a strong economic incentive to act honestly.

Hashed timelock contracts (HTLC) Payment channels solve the problem of transactions only between two participants. But how can a payment be sent to someone with whom there is no direct channel? This is where HTLCs come into play. This mechanism makes it possible to route payments securely through a chain of intermediaries. Suppose Alice wants to send a payment to Dave via Bob and Carol (Alice → Bob → Carol → Dave) [4, 9].

1. Dave generates a random number R and computes its hash H = hash(R). He transmits this hash H to Alice.
2. Alice creates an HTLC contract with Bob: she will pay him if he provides the preimage R for the hash H within 3 days. If not, she will reclaim her funds.
3. Bob, seeing this contract, creates an analogous HTLC with Carol, but with a shorter term (for example, 2 days).
4. Carol creates an HTLC with Dave with a term of 1 day.
5. Now Dave, in order to receive the funds from Carol, must reveal the secret R to her. As soon as he does so, he receives the payment.
6. Knowing R, Carol claims the funds from Bob. Knowing R, Bob claims the funds from Alice.

The payment successfully traversed the entire chain, and none of the intermediaries could steal the funds, since the payment and the revelation of the secret are linked atomically. If a failure occurs at some stage (for example, Carol is offline), then upon expiry of the timeouts the funds simply return to the senders.

Theoretically, HTLCs allow the creation of payment paths of any length. In practice, however, a complex problem of finding an optimal route arises. The sending node must find a path to the recipient consisting of channels with sufficient liquidity to carry the payment. This task is nontrivial because balances in the channels are constantly changing, and this information is not public [3, 5].

Thus, the results of the analysis show that the Lightning Network is a complex, multilayered system that successfully solves the throughput problem while giving rise to a new class of challenges related to network topology, liquidity management, and economic incentives.

DISCUSSION

The LN protocol, while solving the technical problem of transaction speed and cost, creates a new economic reality. Nodes with large amounts of capital and channels naturally become central routing hubs, since payments are more likely to pass through them. This phenomenon, known as the Matthew effect rich get richer, can lead to the formation of a hub-and-spoke topology, where a few large, professionally managed nodes handle the overwhelming majority of transactions. Although this is efficient from the standpoint of routing, such a structure makes the network more vulnerable both to technical failures the outage of a major hub and to censorship.

This dynamics can be visualized in the context of the scalability trilemma. Figure 1 presents the author's interpretation of the scalability trilemma as applied to first- and second-layer solutions. A first-layer blockchain (Layer-1) such as Bitcoin sacrifices scalability in favor of maximal security and decentralization. The Lightning Network, as a second-layer solution (Layer-2), increases scalability. However, this shift creates tension along the decentralization axis. Network efficiency pushes it toward centralization around large, liquid hubs, moving it away from the ideal of a fully distributed network [6, 7].

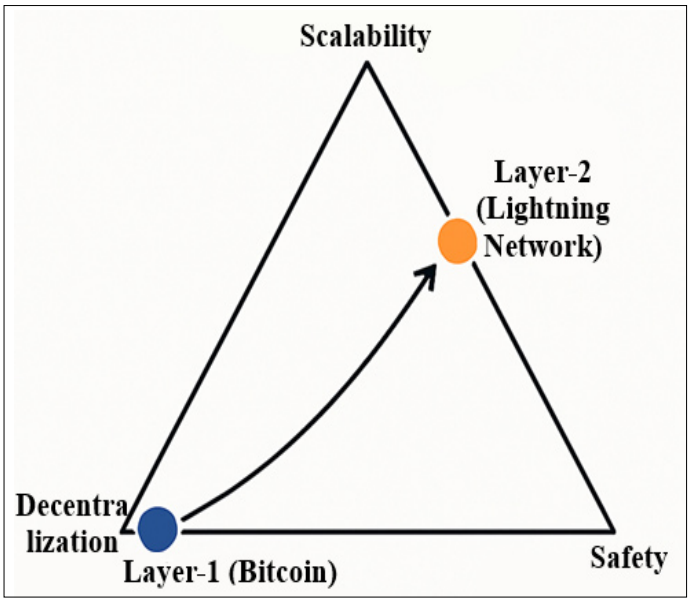

Fig.1. Scalability trilemma in the context of Layer-1 and Layer-2 [6, 7]

Thus, although LN technically remains decentralized anyone can run a node, its economic topology may become centralized. This is not necessarily bad, but this trade-off should be clearly recognized by the community.

To understand the mechanics of the network more deeply, consider the life cycle of a multi-hop payment, which is the foundation of LN operation. Figure 2 presents a schematic of the life cycle of a multi-hop payment via HTLC [8, 10].

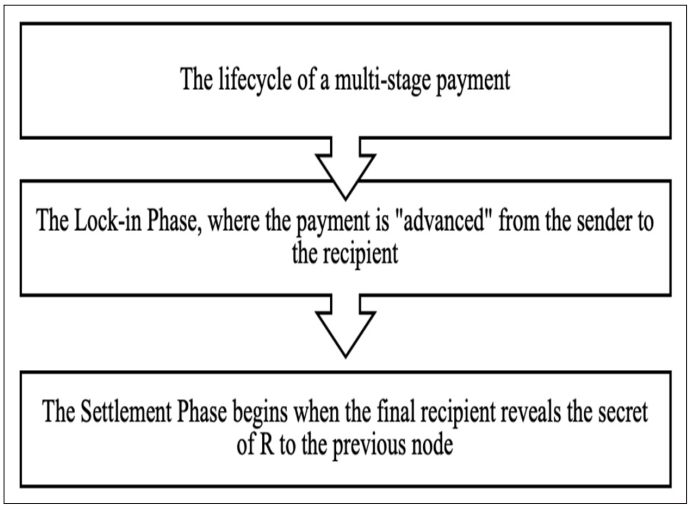

Fig.2. The life cycle of a multi-stage payment [8, 10]

As can be seen from Figure 2, the process consists of two key phases. The first phase – the lock-in phase, in which the payment advances from the sender to the recipient. At this stage, participants create a chain of HTLC contracts with decreasing timeouts, locking funds under the condition of revealing secret R. The second phase – the settlement phase. It begins when the final recipient discloses secret R to the preceding node, which triggers cascading execution of the contracts in the reverse direction. This two-phase structure guarantees payment atomicity: it either reaches the end, or the funds are returned to the sender.

The complexity of this process and its dependence on the availability of all nodes along the path create demand for reliable and always-online hubs. To counteract natural centralization, one can propose hybrid routing models that combine the efficiency of large hubs with the flexibility and resilience of a decentralized network.

Figure 3 presents the author's concept of a hybrid routing model. This model envisages the coexistence of two types of path discovery. Priority routing (Hub-First Routing): For standard payments, the algorithm first attempts to construct a route through well-known, large, and reliable hubs. This ensures high speed and a high probability of success for most transactions.

Exploratory routing: If a path through hubs cannot be found (for example, due to insufficient liquidity), or if the user explicitly selects the option of maximum decentralization, the algorithm switches to a slower but more distributed path search, using protocols of gossip (gossip) to discover less well-known channels [7, 11, 12].

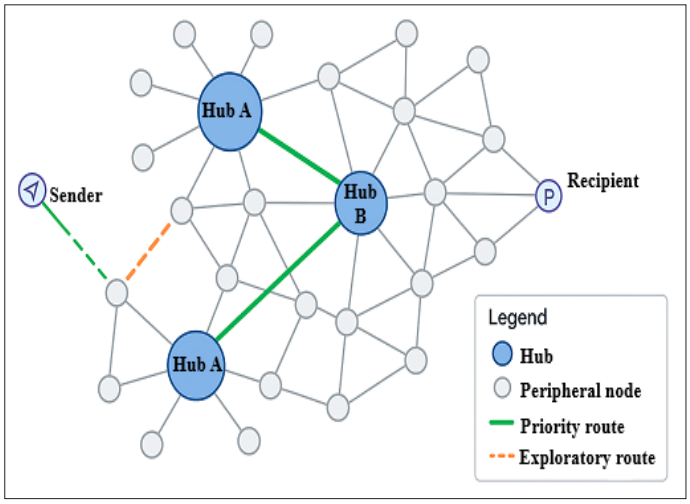

Fig.3. The concept of hybrid routing model in LN [7, 11, 12]

Such an approach would allow users to choose between efficiency and decentralization, and would also reduce the load on the entire network by segmenting traffic.

Lightning Network is a complex system with trade-offs. The discussion of its future should shift from simply praising its speed and low cost to a rigorous analysis of its economic and topological properties. The long-term success of LN will depend on the development of protocol-level enhancements (for example, hybrid routing or improved liquidity management) that can mitigate the tendency toward centralization and preserve the resilience of the network.

CONCLUSION

During this study, the architecture of the Lightning Network protocol and its role in addressing the fundamental problem of blockchain scalability were comprehensively examined. The work achieved its stated objectives and confirmed the proposed hypothesis.

The following tasks were accomplished:

1. Analyzed the limitations of layer-one blockchains: It was shown that the low throughput of networks such as Bitcoin is a consequence of their architectural trade-offs in favor of decentralization and security, which makes them unsuitable for mass micropayments.
2. Described the architecture of the Lightning Network: The components of the protocol were considered – payment channels based on multisignature addresses, commitment transactions with a revocation mechanism to ensure participant honesty, and hashed timelock contracts (HTLC) that enable secure multi-hop payments.
3. Assessed the efficiency and challenges of the protocol: It was established that LN successfully solves the scaling problem, providing the ability to conduct instant and virtually free transactions. At the same time, analysis of the contemporary literature and network topology revealed a number of serious challenges: the complexity of routing algorithms, the problem of liquidity management in channels, and, most importantly, the economic incentives leading to the centralization of the network around large hub nodes.

The analysis corroborates the core hypothesis: the Lightning Network is an effective mechanism for scaling transaction throughput; yet its durability as a genuinely decentralized substrate remains contingent on forthcoming advances that tame path-finding complexity and curb concentration of control. In practice, LN's trajectory hinges on negotiating a workable compromise between the transactional efficiency yielded by well-capitalized hubs and the robustness, censorship-resistance, and fault tolerance characteristic of more diffuse topologies.

More broadly, LN recasts blockchains from slow, high-value settlement rails into a payment fabric capable of sustaining a global micropayments economy. This transformation is not self-executing: it presupposes continuous progress in protocol engineering (e.g., routing and liquidity discovery), incentive design (to discourage centralization and enable sustainable fee dynamics), operational tooling (for rebalancing and risk management), and usability. Only with such sustained architectural and economic refinement will the network realize its promise at scale.

REFERENCES

1. Kim, H. J., Song, G. J., Jang, K. B., & Seo, H. J. (2021, November). Cryptanalysis of caesar using quantum support vector machine. In 2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia) (pp. 1-5). IEEE. https://doi.org/10.1109/ICCE-Asia53811.2021.9641932.
2. Divakaruni, A., & Zimmerman, P. (2023). The lightning network: Turning bitcoin into money. Finance Research Letters, 52, 103480. https://doi.org/10.1016/j.frl.2022.103480.
3. Mizrahi, A., & Zohar, A. (2021, March). Congestion attacks in payment channel networks. In International conference on financial cryptography and data security (pp. 1-25). Berlin, Heidelberg: Springer Berlin Heidelberg.
4. Kappos, G., Yousaf, H., Piotrowska, A., Kanjalkar, S., Delgado-Segura, S., Miller, A., & Meiklejohn, S. (2021, March). An empirical analysis of privacy in the lightning network. In International Conference on Financial Cryptography and Data Security (pp. 1-26). Berlin, Heidelberg: Springer Berlin Heidelberg.
5. Dasaklis, T. K., & Malamas, V. (2023). A Review of the Lightning Network's Evolution: Unraveling Its Present State and the Emergence of Disruptive Digital Business Models. Journal of Theoretical and Applied Electronic Commerce Research, 18(3), 1338-1364. https://doi.org/10.3390/jtaer18030068.
6. Poon, J., & Dryja, T. (2016, January). The bitcoin lightning network: Scalable off-chain instant payments.
7. Zabka, P., Förster, K. T., Decker, C., & Schmid, S. (2024). A centrality analysis of the lightning network. Telecommunications Policy, 48(2), 102696. https://doi.org/10.1016/j.telpol.2023.102696.
8. Pickhardt, R., & Nowostawski, M. (2020, May). Imbalance measure and proactive channel rebalancing algorithm for the lightning network. In 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-9). IEEE. https://doi.org/10.1109/ICBC48266.2020.9169456 .
9. Bartolucci, S., Caccioli, F. & Vivo, P. A percolation model for the emergence of the Bitcoin Lightning Network. Sci Rep 10, 4488 (2020). https://doi.org/10.1038/s41598-020-61137-5.
10. Russell, R., et al. Basis of Lightning Technology (BOLTs). GitHub. Retrieved from https://github.com/lightning/bolts (date of access: 19.07.2025)
11. Guasoni, P., Huberman, G., & Shikhelman, C. (2025). Lightning network economics: Topology. Management Science, 71(7), 5477-5490. https://doi.org/10.1287/mnsc.2023.03872
12. Shcherbina, Y., & Mesyura, V. (2020). Finding the optimal payment route in the Lightning Network. Visnyk of Vinnytsia Politechnical Institute, (6), 93–99.