Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

Bitcoin Layer Two Scaling Solutions: Lightening Payment Channels Network Comprehensive Review, Mechanisms, Challenges, Open Issues and Future Research Directions

Hasan Falah Hasan[1,2], Mohd Najwadi Bin Yusoff [1*], Shams Mhmood Abd Ali[1,3]

[1]School of Computer Science, Universiti Sains Malaysia (USM),
Main Campus, Gelugor, Penang, 11700, Malaysia
[2]School of Engineering, Al-iraqia University,
AlAzhamiya - Haibba Khatoon Street, Baghdad, Iraq
[3]College of Arts, University Al-iraqia University,
AlAzhamiya - Haibba Khatoon Street, Baghdad, Iraq

*Corresponding Author: Mohd Najwadi Bin Yusoff

DOI: https://doi.org/10.52866/ijcsm.2024.05.01.003
Received June 2023 ; Accepted August 2023 ; Available online January 2024.

ABSTRACT: Blockchain technology era is triggered due to current advancement in the decentralized paradigms via facilitating secure collaboration among untrusted entities consequently superseding the necessity for the trusted third parties' existence. Notwithstanding its potential, blockchain scalability faces severe limitations such as low throughput, high fees, and confirmation time latency. Several scaling solutions have been proposed, including layer one solutions that substantially require fundamentally amending blockchain underlying infrastructure resulted in further scalability complications. Layer two solutions, specifically Lightning Network, is a successful cryptographic layer built atop of the Bitcoin blockchain that aims to alleviate these implications by deporting transaction processing outside blockchain while ensuring security and consensus inherited from blockchain without compromising its infrastructure. Payment channels form the core of the lightning network, facilitating fast and secure transactions between participants. However, the network encounters substantial obstacles associated with transaction amounts that exceed the current channel capacity, leading to payment failures and limiting its effectiveness. Payment Channel Networks (PCN) have been risen as an evolved replacement that solves payment channel's issues, seeking to enhance transaction throughput and reduce confirmation delays by solving limited capacities shortages. This paper thoroughly examines PCN efficiency impacting factors that hinder its current adoption growth and avoiding its widespread employment. Additionally, existing solutions are reviewed and categorized based on the PCN building architecture. The research concludes by outlining potential research avenues and future directions to improve the efficiency and practicality of the Lightning Network PCN. This research contribution aids the advent of blockchain layer two technology and participates in its integration into real-world applications.

Keywords: Blockchain, Layer Two Solutions, Lightning Network, Payment Channels Network, Efficiency Challenges.

1. INTRODUCTION

Blockchain is a decentralized digital public ledger that enables secure recording, storing, and verification of transactions across multiple nodes in a network [1]–[3]. It was built as cryptocurrency foundation storing technology such as Bitcoin nonetheless, the demand on its services have been extended to other industries. At its core, it comprises numerous components like consensus mechanisms, miners and interconnected blocks containing a set of transactions. The consensus mechanism is the regulator that organizes transactions validation processes and new blocks addition to

the chain accompanied with guaranteed integrity, immutability, decentralization, transparency, and trustlessness therefore, the selection of a specific consensus mechanism relies on the blockchain predefined objectives. Proof of Work (PoW) is employed by the Bitcoin blockchain. Miners aim to solve complex mathematical puzzles, leading to the first successful miner earning the privilege of adding a new block to the blockchain; however, despite its effectiveness, this process is highly costive in terms of energy consumption. Proof of Stake (PoS) offers an energy-efficient alternative and is exemplified by Ethereum blockchains. Validators are chosen to create blocks and verify transactions based on the amount of stake they have. Delegated Proof of Stake (DPoS) featured in blockchains like EOS and Tron, introduces a voting system where token holders select a limited number of delegates. These delegates are responsible for validating transactions and creating new blocks, boasting scalability and speed as their strengths. Proof of Authority (PoA) states that validators are identified entities which operate in private and consortium blockchains where trust is guaranteed.

Proof of Space (PoSpace) allocates storage space to miners for their participation in the consensus process. Miners must prove they have reserved a specific amount of disk space, showcasing a more energy-efficient alternative to PoW. Proof of History (PoH) employed by Solana's blockchain to timestamp transactions without the need for miners to solve intricate puzzles resulting in rapid throughput and swift confirmation times. Practical Byzantine Fault Tolerance (PBFT) is a favored choice for permissioned, relying on a predefined set of nodes to efficiently reach consensus due to its obvious efficiency. Miners are powerful elected mining nodes which are responsible for verifying transactions by relying on their powerful capacity and resources through solving complex puzzles suggested by a consensus mechanism. Once transactions are verified, the consensus algorithm will incorporate them into the block, ensuring that all networked participants unanimously agree on the transactions' validity and, thus, immutability and finality are attained [4]. Finality is an essential concept as it operates in common blockchain networks. It refers to the point at which a transaction is considered irreversible and confirmed. However, in most blockchain networks, finality is achieved probabilistically. It states that as more blocks are added to the blockchain, the likelihood of a transaction being reversed or altered diminishes significantly. Each additional block added to the chain further solidifies the transaction's status, making it exponentially less likely to be subject to a blockchain reorganization or fork. Upon appending a block to the chain, it becomes an enduring and transparent record that is difficult to modify.

Decentralization is a crucial feature that eliminates the need for any central authority to validate and authorize transactions. Instead, it relies on a network of distributed nodes, working together to ensure the system's integrity and immutability through storing a copy of the ledger locally. It enhances transparency, security, and resilience. Furthermore, Its potential to revolutionize various industries such as supply chain management, healthcare, voting, intellectual property protection, and many others have benefited from its services [5]–[8]. However, due to security and decentralization features, scalability remains a major drawback in which low transaction throughput is estimated to be 7-10 tps, high verifying fees at peak times, while confirmation and inclusion consumed time is elevated, reaching 60 minutes caused by the consensus algorithm [9]. It is proven that Bitcoin consumes 3373287.7–34817351.6 global kWh while 360.39300–3691.40700 is exact (kWh/per transaction) [10]. Blockchain trilemma was addressed initially by Vitalik Buterin, the founder of the Ethereum blockchain, stating that scalability, decentralization, and security properties cannot be all enhanced simultaneously to the full extent while emphasizing achieving balanced solutions among these features [10]. Several scaling solutions have been introduced in the blockchain. Layer one solutions, like Hard Fork, were proposed to amend block size while it impacts security. Additionally, a segregated witness has been introduced to remove signatures from the transaction's structure, enhancing storage spaces, leading to better scalability while influencing security passively. Finally, sharding that segments blockchain into several storing clusters and controlled by certain shards; however, it dedicates centralization that in essence violates decentralization nature.

Layer one solutions are yet to be efficient due to substantial amendments to blockchain underlying infrastructure, leading to high costs incurred [11],[12]. Layer two emergence such as Lightning Network represents a promising solution that scales blockchain. It is a cryptographic protocol that functions atop the Bitcoin blockchain. Lightning Network's primary purpose is to alleviate transaction processing burdens from the blockchain without compromising the blockchain’s infrastructure; meanwhile, it inherits only security and consensus. It is formed mainly by Payment Channels by connecting two users who are required to contact the blockchain in three cases: open, close, and dispute cases. In an open case, users contact blockchain to open a shared account with deposited funds by both sides with mutually signed transactions to regulate how the fund will be spent. Closing channel is incurred once the payment lifecycle is finished or channel capacity is depleted, and final balances are updated and published in the blockchain. Finally, in dispute cases rises in which blockchain with supported evidence to preserve victims’ rights. However, transferring amounts that exceed the channel capacity within the current design can result in payment failures. Additionally, channel availability is affected, and the lack of support for rebalancing further impacts overall efficiency. Payment Channel Networks (PCN) has been

devised by Poon and Dryja in 2016 [14] as a promising, efficient, and scaling solution to overcome the payment channel's capacity by concatenating several available channels, forming an indirect payment path among participants devoiding of opening new channels, and avoiding blockchain costive processes.

PCN relies on splitting big amounts into several micropayments, first introduced by Piatkivskyi and Nowostawski in 2018 [15]. Payment splits are routed among communicated participants versus small paid fees; however, split delivery is not guaranteed; therefore, a conditional transfer mechanism rises as persistence demands to achieve synchronized payments. Despite the promising advantages of PCN, many questions remain unanswered. There is a noticeable deficiency in detailed studies that explore the workings, existing challenges, and potential issues that might emerge avoiding its wider usage. Furthermore, there is a clear need for focused pathways to guide future research addressing these concerns and facilitating a smooth integration of Layer Two solutions within the existing blockchain framework. As far as we are aware, no previous research has conducted a thorough analysis evaluating the PCN efficiency-impacting factors or categorized solutions based on the mechanism's architecture. This research bridges the current knowledge gap through an in-depth examination of the PCN, delving into its operational mechanisms, identifying ongoing challenges, and highlighting unresolved issues through a comprehensive review that formulates, identifies, classifies, and defines the factors influencing PCN efficiency while categorizing solution mechanisms based on their architecture. Simultaneously, it identifies and distributes literature related to PCN efficiency factors. By addressing these challenges, we aim to advance scalable blockchain solutions, unlocking the full potential of blockchain technology across various industries. Our goal is to provide a robust roadmap for future research, facilitating the sustainable growth and adoption of Layer Two scaling solutions. The remainder of this paper is organized as follows; Section 2 considers the proposed research taxonomy, while section 3 includes layer two solutions. Section 4 includes interoperable mechanisms that currently built solutions and their evolutions; furthermore, section 5 represents PCN, its architecture, synchronization and efficiency impacting challenges. Sections 6 and 7 formulate and classify recently proposed solutions.

2. RESEARCH TAXONOMY

The proposed taxonomy is explicitly dedicated to analyzing Bitcoin blockchain layer two solutions through navigating a Lightening Network incorporated with current investigated channels in terms of their evolution, types, interoperable mechanisms, solutions, synchronization, especially HTLC, efficiency impacting factors, and finally, solutions categorization as depicted in Figure 1.

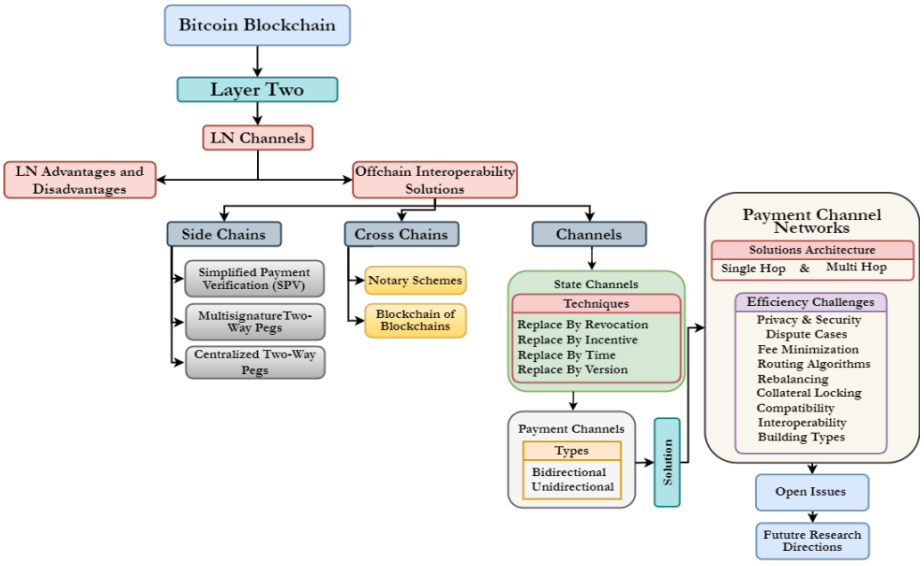

Figure 1. - Research Taxonomy.

3. LAYER TWO

Layer Two solutions often called off-chain, are protocols built to enhance Bitcoin blockchain scalability and efficiency by addressing particularly transaction throughput and time latency limitations. Solutions have achieved this by processing certain transactions off-chain, reducing the burden on the main blockchain while maintaining security and trustworthiness. Lightening Networks (LN), Side Chains and many others are prominent examples currently employed

for more practical and everyday transactions, microtransactions, and a wide range of applications beyond simple peer-to-peer payments. The LN was first introduced in 2016 by Poon and Dryja [14] as a cryptographic application designed to overcome the scalability aforementioned limitations. Figure 2 depicts simple LN architecture.

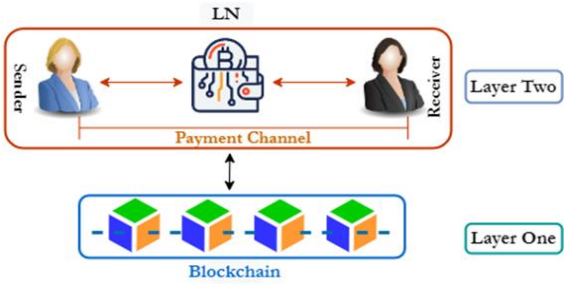

Figure 1. - LN Building Concept.

The primary goal of the LN is to enable fast, secure, and cost-effective transactions in a trustless manner within a peer-to-peer network of payment channels. It utilizes state and payment channels as its core components. Payment channels are dedicated to financial purposes, while state channels provide a generalized channel usage concept. It forms an offchain of networked channels separate from the Bitcoin blockchain. Unlike traditional Bitcoin transactions that are only broadcasted, LN employs specific communication protocols and routing algorithms to route transactions. Combining on-chain and off-chain allows the LN to scale the blockchain without requiring fundamental changes to the underlying infrastructure or consensus mechanism [16]. Participants establish payment channels with one another, conducting multiple transactions securely and without broadcasting each transaction in the blockchain as it significantly reduces transaction fees and processing times, increasing overall transaction throughput. Participants create and sign a smart contract in a payment channel, defining the rules for the channel's operation regarding depositing and spending funds. State channels extend beyond financial services and offer advantages in various applications across different industries such as gaming, healthcare, management, content delivery networks and many others. In LN, state channels act as indicators for updating the channel state, with multiple parties collectively agreeing on new states for previously agreed-upon smart contracts. Over time, channels have evolved from unidirectional to bidirectional, enabling both parties to send and receive payments [16]–[18]. They have further evolved into multihop and singlehop networks [20], [21], enhancing the overall network's scalability and flexibility.

Table 1 highlights the advantages and disadvantages of LN. Intensive researches have resulted in various off-chain protocols aimed at enhancing the efficiency and scalability of LN by addressing other impacting factors, which will be discussed in later sections. These protocols include payment channels [18],[21], [22], virtual channels [24], channel factories [25], payment channel networks [13],[25]–[27], routing protocols [28],[29], fee minimization [31], reduced collateral time locking [32], channel rebalancing [33], as well as security and privacy enhancement [33]–[35]. These protocols leverage essential blockchain properties like integrity and synchronicity, performing efficiently within specified time windows [36],[37].

Table 1. - LN Advantages and Disadvantages.

Advantages		Disadvantages	
Fast Payments	There are no inherent restrictions on the number of payments per second, while the only limitation is the capacity of the channel. [36].	Security	• Centrality arises from interconnected channels featuring well-equipped nodes, channel capacity, availability, and the dynamic nature of routing mechanisms. [20]. • It does not support security generating proofs [39].
Trustless Transactions	There is no need for trusted third parties; therefore, decentralization and autonomy	Anonymity	One of the obstacles is to preserve identities and capacities that aim to remove any linking relation and avoid the impact of several attacks [40].

	are ensured in payment processes [22].		
Cost-Effective Fees	Cheaper transaction processing in LN compared to on-chain Bitcoin transactions [41].	Closed Channel Fraud	One of the risks when using the LN is closing the channel and going offline through fraudulent channel close [39].
Open Indefinitely	Channels can remain open indefinitely if both parties cooperate [42].		
Scalability	High transaction throughput can process millions of transactions while channels remain open [23].		
Atomic Swaps	Ability to route payments across multiple compatible blockchains [43].		
Privacy	Payments are not publicly recorded in the blockchain, enhancing privacy. [40] [36].		
Low Resource Consumption	Requires fewer resources and incurs less computation overhead, as information is not stored indefinitely [44].		

4. OFF-HAIN INTEROPERABILITY MECHANISMIS.

It refers to the set of protocols, technologies, or methods used to facilitate communication and interactions between different blockchain networks or between blockchain and non-blockchain systems in an off-chain mode without conducting all of the operations on the main blockchain. The role of off-chain interoperability mechanisms is to enable data transfer, value exchange, or information sharing between multiple blockchain networks or systems efficiently and securely. This is crucial because the blockchain ecosystem is highly fragmented, with various blockchains designed for different purposes and use cases. Interoperability mechanisms allow these blockchains to work together and leverage each other's strengths while maintaining security and trust. Consequently, Off-chain interoperability mechanisms play a vital role in connecting and coordinating the activities of different blockchain networks and systems. They help overcome the challenges of fragmentation and isolation in the blockchain ecosystem, allowing for a more interconnected and versatile blockchain space.

4.1 SIDECHAINS

Sidechains have revolutionized the blockchain space, offering significant advancements in interoperability and scalability; meanwhile, security and privacy features are enhanced, resulting in contributing to the evolution of existing blockchains [29]. Their primary purpose is to expand the capabilities of interconnected blockchain networks, enabling seamless data transfer and reinforcing overall system security, as shown in Figure 3.

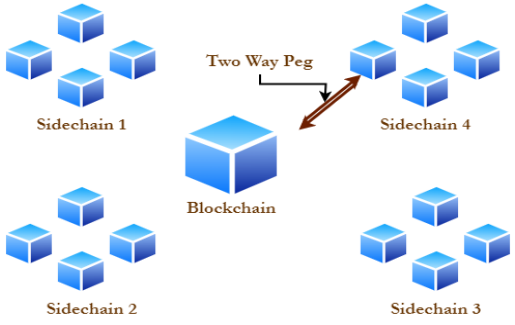

Figure 2. - Side Chains Architecture.

One of the critical benefits of sidechains is their ability to be isolated from the on-chain, safeguarding against cryptographic vulnerabilities. Any security issues arising in a sidechain are contained within its environment, protecting the on-chain. They enable decentralized token transfers and data exchange between different blockchain systems, achieved through specifically designed chain structures and consensus mechanisms through utilizing different consensus protocols, providing greater flexibility. They are connected with the on-chain via a two-way peg mechanism, enabling smooth data and consensus transfer between the two blockchains. Users can lock their tokens on the on-chain, and the sidechain generates an equivalent value of tokens for its ecosystem. Conversely, users can transfer tokens between the sidechain and the on-chain, resulting in a corresponding adjustment of tokens. Sidechains architecture is typically classified into three types of schemes, as represented in Table 2 [44]–[46].

Table 2. - Side Chains Solutions.

Scheme	Methodology
Centralized Two-Way Pegs	This straightforward approach relies on a trusted third party to oversee token locking and unlocking operations between the on-chain and pegged sidechains. Third-party manages these operations on both chains.
Multisignature/Federated Two-Way Pegs	An enhanced iteration of centralized pegs, this approach involves a group of notaries controlling the lockbox. Token transfers require the majority agreement of the participating notaries.
Simplified Payment Verification (SPV)	SPV, also known as lightweight clients, enables transaction verification without downloading the entire blockchain. It uses Merkle tree proofs to validate target transactions and ensures the security of the sidechain. The process involves waiting periods for confirmation and contest, eliminating the need for third parties.

4.2 CROSS CHAINS

Cross chains are crucial in facilitating asset transfers between blockchains by establishing a communication medium. However, moving assets from a blockchain with a less secure consensus mechanism to one with a more robust mechanism can introduce safety risks due to the differences in their respective security measures and protocols. Figure 4 provides a conceptual overview of cross chains [43], [48].

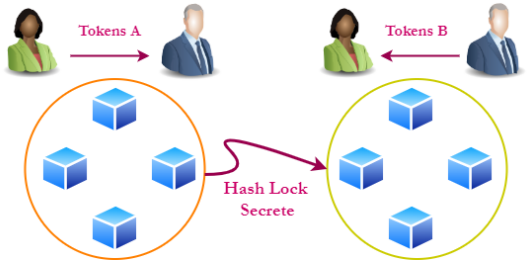

Figure 3. - Cross Chains Conceptual Overview.

A standard Cross Chain Communication protocol comprises three main phases: commit on chain A, verify and commit on chain B, and an optional abort. The central challenge is represented by the required design to establish the appropriate trust model for each phase by considering whether relying totally on a trusted third party, dependence on an explicit synchrony assumption, or a hybrid approach that involves a trusted third party only when synchrony is breached. In the Pre-Commit Phase, the commit step typically involves locking and unlocking assets on chains A and B based on protocol outcomes. Coordinator implementations are classified based trusted model. Trusted third-party coordinators are the simplest approach which correct execution, involving custody of assets and participation in blockchain consensus, while synchrony assumptions replace coordinators, with participants independently verifying commitments within a specific time frame. Finally, a hybrid model that represents a combination of both trusted models, watchtowers is a perfect example that acts as a fallback to ensure correct termination. In the verification phase, the commitments on interlinked chains can be verified under various trust models. These include relying on a trusted third party for simplicity, using synchrony assumptions for direct observation or chain relay intelligent contracts, or adopting a hybrid approach combining synchrony and a trusted third party. The Abort Phase often applies to exchange protocols. In this phase, approaches vary based on trust models. Trusted third parties can handle aborts, or timelocks can be introduced for

protocol termination. A hybrid approach involves using watchtowers to ensure correct termination if participants experience failures. The notary schemes and blockchain of blockchains act as intermediary platforms for facilitating inter-blockchain transactions [49], [50], as illustrated in Table 3.

Table 3. - Cross Chain Types.

Chain Type	Working Methodology	
Notary Schemes	Notaries actively monitor multiple blockchains and listen for transaction events, enabling interoperability and seamless asset transfers between different blockchains. When a relevant event occurs on one chain, the notary creates a corresponding transaction on another chain. Crypto exchanges like Binance and Coinbase exemplify this notary concept [51].	
Blockchain of Blockchains	This approach aims to achieve interoperability and customization by connecting several interconnected blockchains that securely share data managed by a central chain. It focuses on reducing blockchain development periods to the shortest possible duration. Two proposed solutions are Cosmos and Polkadot [17].	
	Cosmos	**Polkadot**
	Independent blockchains are connected in a decentralized manner, each called a zone and having its own rules to manage its assets. Zones are connected using a bridge-hub model, where each hub serves as a central point for sharing state updates, forming a network of zones.	The concept of Parachains, where coherent parallel chains exist alongside the main blockchain. Validators in the main chain validate state transitions, while interparachain communication is facilitated through the Cross-Consensus Message Format (XCM) and Cross-Chain Message Passing (XCMP) protocols. Polkadot allows for the direct connection of numerous parachains to the relay chain, though long-term connections and nested parachains are still in development.

4.3 CHANNELS

Channels are a fundamental infrastructure component that enables off-chain transactions applicability. They are a mechanism through which participants can interact and conduct multiple transactions without the need to record every single transaction on-chain. They are a way to facilitate fast and cost-effective Bitcoin transactions; meanwhile, state channels are more versatile than payment channels. While payment channels are designed primarily for payments, state channels allow participants to engage in complex, multi-step transactions, similar to smart contracts on-chain. In essence, payment and state channels are the engines driving the LN, enabling fast Bitcoin transactions while addressing scalability, privacy, and efficiency challenges.

4.3.1 STATE CHANNELS

It has broadened the payment channel concept, enabling application diversity [23]. These channels offer a lightweight solution for scaling layer two transactions by conducting offchain transactions between parties. Payment channels evolution is elevated by state replacement techniques, which assume rational behaviour and adherence to agreed-upon obligations by channel participants [52]. Two smart contracts are utilized in state channels: one for the state channel and the other for the application execution. State replacement techniques ensure that channel states are updated on-chain. Parties exchange signed messages with updated states and round numbers. If a party fails to respond or provide invalid data, a dispute can be initiated by broadcasting the recently agreed state on-chain. The dispute handler verifies evidence during a waiting period and commits the state with the highest round number. After finalizing the state, participants can submit new inputs for the subsequent round [36],[52]. State Replacement Techniques (SRT) represent controlling techniques to ensure the channel's evolution by replacing the old state with a new state. Ideally, state replacement should occur once to achieve transaction finality. However, certain state replacement techniques incorporate a dispute mechanism to address potential participant disagreements regarding the proposed new state [54]. Table 4 presents the state replacement techniques.

Table 4. - State Replacement Techniques.

Techniques	Roles
Replace by Incentive **(RbI)**	Transaction sender signs and announces a new state while the receiver needs to countersign it, motivating him by offering higher incentives [39], [55].
Replace by Timelock **(RbT)**	State channels have associated timelocks based on blockchain block height. As time passes, timelocks decrease. Before expiry, newer states replace older ones. The state with the lowest timelock is included in the blockchain first. Expired timelocks make transactions immutable [17].
Replace by Revocation **(RbR)**	Participants may need to revoke a previously submitted state on the blockchain. To do this, all participants must propose a new state within a specified time window determined by the parent blockchain [56].
Replace by Version **(RbV)**	An incrementing counter indicates the version of a state. A higher version number denotes a more recent state. Therefore, a higher state number can replace an older state [52, 56–58].

The RbI and RbT mechanisms ensure that the latest state is inserted into the blockchain only once, maintaining data integrity. Conversely, the RbR and RbV mechanisms allow participants to challenge the submitted state through a dispute process, where counterevidence can be provided. This dispute process can lead to either a closure or a command dispute. In a closure dispute, the channel is closed, and the resolution occurs exclusively on the underlying blockchain. The relevant parties must submit evidence within a predetermined time frame. After the evidence is submitted, one of the participants processes the evidence to resolve the dispute. [23],[59]. In contrast, command disputes execute a set of commands on the parent chain to resolve disputes, and the channel resumes its operation offchain after command execution. The blockchain provides a fixed time duration to collect commands from the participants and executes all the collected commands to find a resolution [59]. Some solutions, such as [19],[60], extend the dispute process expiry time to support the execution of a large number of commands [61]–[63]. However, both dispute resolution mechanisms always assume the relevant participants to be online. To address the need for continuous online participation, watching services assist participants in observing disagreements, subverting the requirement of staying online, thereby, cost overhead rise as an implication issue.

4.3.2 PAYMENT CHANNELS

Payment channels are a solution for faster and more scalable transactions in the LN, as they enable users to conduct multiple transactions without involving the blockchain directly for each transaction. Participants in a payment channel can establish it by opening a multi-signature account with a predefined amount representing the channel's capacity, while funding and refunding transactions are required to be signed prior to the payment process performed in order to regulate spending regulations. Once the channel opens, it can perform unlimited offchain transactions, updating its balance state regularly. The final channel state is recorded on the blockchain when the participants decide to close the channel. This approach reduces transaction fees, improves transaction speed, and enhances scalability compared to traditional on-chain transactions [56]. However, channel capacity and the necessity for direct connections solely between two parties pose a notable efficiency obstacle, especially when the transaction amount exceeds the channel's current capacity, resulting in payment failures. Moreover, the absence of support for payment channel rebalancing contributes to a reduction in available channels caused by issues such as channel closures, refunds, and channel reopening, all of which are subject to on-chain scaling constraints. These shortcomings have a substantial adverse impact on overall efficiency. [18], [24], [25], [64]. There are two channel types represented in Table 5.

Table 5. - Payment Channel Types.

Channel Type	Specification	Drawback
Unidirectional	It enables one-way fund flow from sender to recipient using two transactions: payment increase and refund. It utilizes RBI technique, with the receiver broadcasting the final settlement transaction for example Spilman channel [66] is a trustless payment channel involving funding and refund	• It does not support conditional payments. • Lacks a mechanism to refund the remaining amounts to the sender. • Transaction malleability allows modification of transaction identification hashes [53, 56].

Bidirectional	transactions, with the channel's lifetime determined by the refund transaction's lock time. Blockchain payment transactions use time locks to settle newer transactions within a shorter window, with a safety margin Δ. Authors in [67] introduced Duplex Micropayment Channels (DMC) combining RbI and RbT through Invalidation Trees. DMC enables bidirectional payments using the lowest time lock branch for blockchain priority. An alternative DMC version supports multiple parties with indefinite channel lifetimes, eliminating fixed expiry times.	• Conflict between channel resets and required branch nodes in disputes. • Computation time. • Payment synchronization. • Privacy and security preserving.

5. PAYMENT CHANNEL NETWORK

PCN was initially proposed by Poom and Dryja [14] as a promising scaling solution to overcome the drawbacks of payment channel capacity. PCN enhances payment channels' lifecycles and optimizes their capacities by creating a network of interconnected payment channels between participants that enable fast, low-cost, and scalable off-chain transactions, ultimately forming an indirect payment path. The primary objective of PCN is to eliminate the need for creating new channels, thereby reducing fees and time consumption associated with regular on-chain processes [17]. PCN facilitates direct and indirect interactions between parties, employing underlying or specifically designed routing algorithms. A crucial concept in PCN is the splitting of large amounts, which was first proposed by [15]. This approach effectively addresses capacity issues by multipath routing algorithms to divide a large payment into several smaller segments. By distributing the payment value across multiple paths, the network can efficiently utilize available channel capacities, increasing the likelihood of successful routing. These split payments can be routed directly from the sender to the receiver based on available channel capacity or indirectly through multiple intermediate hops, accompanied by small charging fees [27]. The success of routing payments in PCN relies on finding suitable paths with sufficient capacities. While PCN mitigates the need for frequent rebalancing, it does not entirely eliminate it [33]. However, the severity of rebalancing in PCN is generally less compared to regular payment channels, ensuring more extended channel availability periods. Despite the benefits of PCN, there are challenges to consider.

Payment splits are not guaranteed to be successfully delivered to the receiver, leading to potential false claims of non-receipt by any participating party. At the same time, the sender remains uncertain about the completion of the payment round. Additionally, transaction finalization time and payment routing paths can be prolonged, causing channel capacities to remain locked and impacting overall channel availability and efficiency. Channel synchronization has been developed to address these challenges [16], [38], [53]. Figure 5 illustrates the lifecycle of PCN.

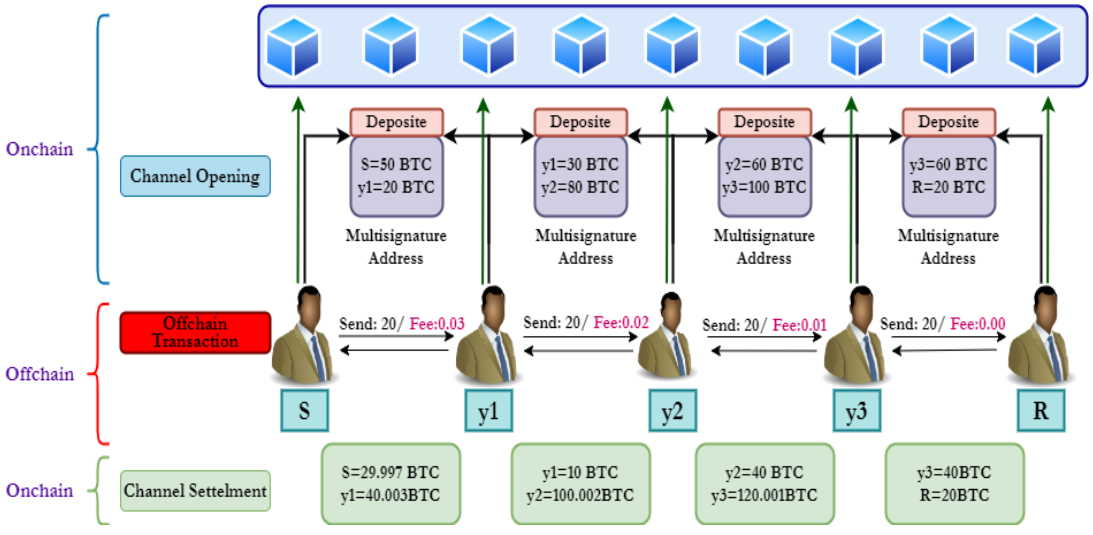

Figure 4. - PCN Lifecycle.

5.1 CHANNEL SYNCHRONIZATION

Channel synchronization, or conditional transfer, is a set of predefined rules agreed upon by communicating parties for transferring specific amounts within a specified time window. Poon and Dryja [14] have defined two fundamental features, atomicity and counterparty risk. They play a vital role in managing and measuring the success of a payment round within the PCN. These backbone properties are essential for forming a secure and efficient conditional communication payment protocols [34]. Table 6 illustrates the required features to achieve channel synchronization.

Table 6. - Channel Synchronization Features.

Feature	Roles
Atomicity	Atomicity is a crucial feature in PCN, ensuring that all sent payments are either fully delivered within a reduced time window or the entire payment process fails window [68]. It guarantees the integrity and reliability of transactions, preventing reserved capacities and allowing termination in case of unresponsive nodes. Better atomicity can be achieved with single-path routed payments and mechanisms like HTLC [68, 69].
Counterparty Risk	Counterparty risk in PCN refers to the possibility of participants defaulting on their obligations. Cryptographic commitment protocols and smart contracts provide added security, ensuring all parties fulfil their commitments and reducing counterparty risk. Balance security (BS) protects participants' funds by maintaining CS, preventing financial losses even with corrupted parties involved [70, 71].

5.2 HASH TIME LOCKING CONTRACTS

Hashed Time Locked Contracts (HTLC) is a cryptographic communication protocol designed specifically for PCN to enable conditional payments between interconnected channel participants within a specified time window [34],[48], [72]–[74]. HTLCs are encrypted smart contracts in the network layer [76], integrated into PCN to form payment paths involving multiple channels, such as LN or DMCs [39],[76],[77]. By enforcing atomicity, HTLC enables cross-channel conditional transfers, where the sender locks coins along a path to the receiver, redeemable only if contract conditions are met. HTLCs rely on two major conditions: Hash Locks (HL) and Time Locks (TL). Table 7 explains the role of both HTLC conditions.

Table 7. - HTLC Conditions.

Conditions	Role
Hashlock (HL)	HL restricts spending of an output until specific data is revealed, allowing multiple outputs with the same HL to be spendable together.
Timelock (TL)	TL restricts Bitcoin spending until a predetermined future time or block height, ensuring contract execution within the network.

HTLC earliest lightweight version relies on the receiver side by generating a preimaged hash value R = H(x) that is built based on a collision-resistant one-way hash function where x is a randomly generated number. Source routing payment is a sender-centric model where the sender has full knowledge of LN nodes, paths, and capacities. The sender manages the payment path, generating and distributing secrets to other participants. The receiver receives a security parameter for contract correctness during secret initiation [43],[78]–[80]. Despite its advantages, source routing payment in PCN suffers from privacy and security issues due to using similar HLs in all routed contracts, disclosing sender-receiver relationships, and exposing transaction values, enabling adversaries to distinguish concurrent payments by corrupted or honest but greedy hops [4],[81]–[83]. Corrupted hops, introduced by external adversaries, aim to disclose transaction history, while honest but greedy hops exploit their power to reject passing small payments [16],[17],[25],[54]. Corrupted hops can share information with a controlling adversary, leading to attacks like analytical and balance discover attacks, violating atomicity [84],[85]. Moreover, channel locking counterparty's capacity and honesty verification mechanisms are lacking, making collusion possible when secrets are revealed in reverse order during payment delivery, leading to being vulnerable to certain attacks such as wormhole attacks and consequently impacting efficiency [70],[86],[87]. Figure 6 represents both HTLC versions.

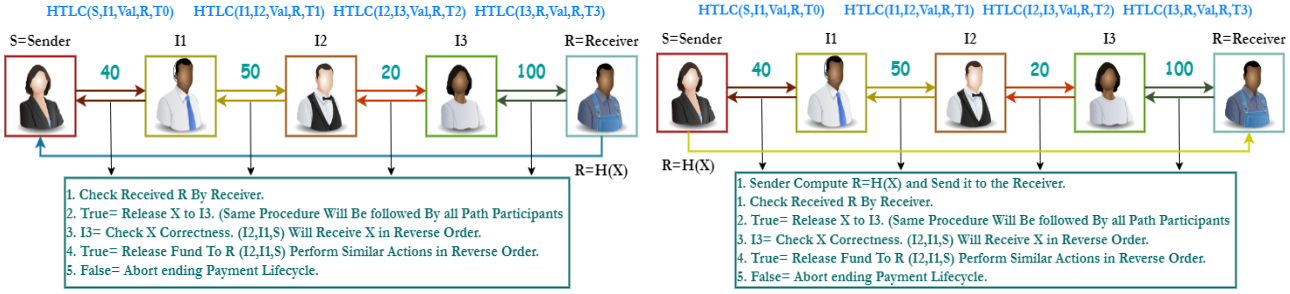

Figure 5. – (a) Earliest Version.; (b) Source Routing

5.3 PCN EFFICIENCY CHALLENGES

Efficiency remains an obstacle that prevents PCN wide adoption due to its fluctuated nature resulting from several affecting factors; which enhancing these factors can be achieved by an adequate balance among them, resulting in reducing measures like computation time, communication overhead, consumed resources, and increasing transaction success rates which warrant careful consideration for its widespread adoption and successful implementation in real-world applications thereby, mature understanding with further developed tools yield to better efficiency [88]–[90]. Figure 7 illustrates currently classified and discussed challenges.

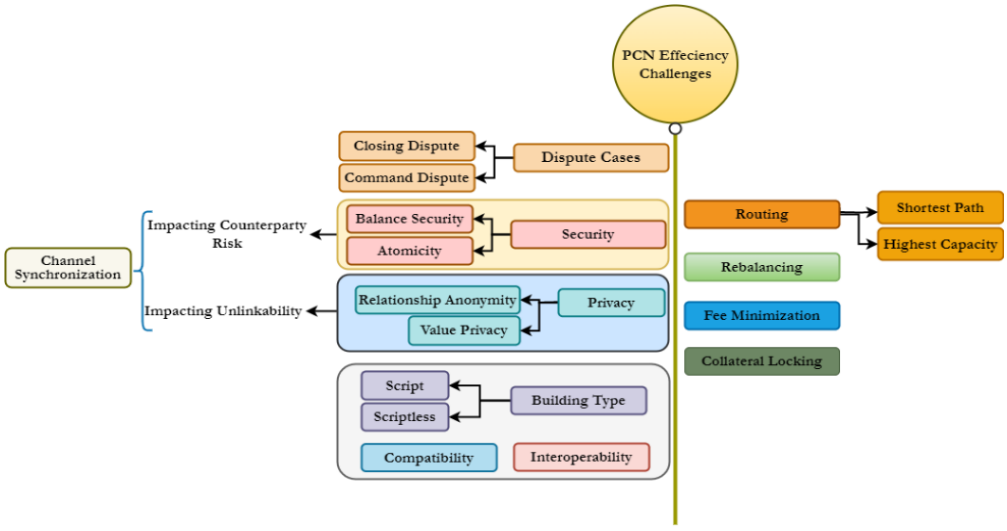

Figure 7. -PCN Efficiency Challenges.

5.3.1 PRIVACY

Ensuring privacy in layer two transactions presents significant challenges, as it requires safeguarding payment history, sender-receiver relationships, sender privacy, and the indistinguishability of concurrent payments. These privacy measures are crucial for preserving participants' identities and their payment history [37],[39],[43]. Meanwhile, preserving transaction privacy is critical in maintaining user privacy and avoiding conflicts with PCN efficiency. It has been proven that privacy is supportive and not a conflictual rival. Privacy disclosure leads to longer transaction finalization times or unresolved transactions, resulting in tied-up assets and reduced channel availability. Moreover, payment rejection can be deliberately made by a rival adversary. In contrast, users face obstacles in completing transactions, impacting the reputation of the payment protocol or nondeliberate due to some participants' greediness to maximize profits, which imposes further implications [91]–[93]. Extensive research has been conducted, and the subsequent sections will explore and analyse the latest proposed solutions. Table 8 provides an organized overview of the privacy measures necessary for layer two transactions.

Table 8. - Privacy Measures.

Measure	Role
Off-Path Value Privacy (VP)	Ensuring the confidentiality of payment history balances to prevent external observations from accessing sensitive information and achieving overall payment privacy [95].
On-Path Relationship Anonymity (RA)	Refers to the requirement that concurrent payments within a payment round should not be distinguishable from each other to maintain anonymity and confidentiality [29].
Sender Privacy	In the context of the source routing concept, the sender's identity must be kept anonymous to protect their confidentiality [16].
Sender-Receiver Relationship	This principle dictates that identities must be concealed during payment processing while the transacted payments are known, necessitating the implementation of VP to preserve privacy [20].

5.3.2 SECURITY

Conditional transfer also has an impact on efficiency. HTLC uses similar Hash Locks (HL) as payment transferring conditions, atomicity is compromised, and the automatic unlocking of all forward contracts can lead to collusion and result in WA [71],[72],[89]. Other cryptographic commitments are either heavy, complex, or crucial to achieving channel consistency. Channel Consistency (CS) ensures contracts include unique cryptographic conditions, requiring each party to pass the revealed secret to its next neighbor to claim funds. By incorporating these features, efficiency is supported by security [29].

5.3.3 DISPUTE RESOLVING

Disputes originated in PCN typically within the network itself but are ultimately resolved on the layer one blockchain [15],[27],[57],[95]. These disputes can arise when a party attempts to deceive others by submitting an outdated transaction state to gain unauthorized access to previously acquired funds or when a party becomes unresponsive and unexpectedly disconnects from the network. Synchronous communication is employed on the layer one blockchain to handle such disputes, allowing parties a specific response timeframe [52],[96]. However, synchronous communication with the on-chain layer poses challenges. Dispute transactions are treated like regular transactions in the on-chain transaction pool, making them subject to the same time and cost constraints, including potentially high fees during peak periods imposed by miners. The pool of pending transactions can contain both valid and invalid ones. Valid transactions include regular on-chain or off-chain transactions, while invalid transactions may result from various attacks, such as the Flood&Loot attack discovered by [98]. This particular attack aims to flood the on-chain network with invalid states, potentially leading to unresolved disputes within the designated timeframe and, consequently, causing a loss of assets for their rightful owners [16],[52],[58],[67].

5.3.4 FEE MINIMIZATION

One of the significant benefits of the PCN is the ability to route payments with low fees. This feature allows all transactions to be transferred at affordable costs, incentivizing the hops in the payment path to act responsibly[19],[98]. As they receive rewards, it helps grow their capital and generates the potential for higher returns. The availability of low fees encourages participants in the payment path to conduct more transactions, ensuring a continuous flow of rewards, which, in turn, contributes to the sustainability of the channels and prolongs their lifespan. However, the design of low-fee algorithms remains challenging, as there are currently no standardized or universally accepted blueprints for minimizing fees [100].

5.3.5 ROUTING

Routing algorithms are essential in impacting PCN efficiency, as they determine whether to prioritize short paths or capacities depending on the specific technique used. It is a significant component for forwarding payments among participants in the network [20],[100]. However, the design of routing algorithms can vary in their advantages and disadvantages. Some algorithms may provide high security but prove to be inefficient, while others might be efficient but less secure [93],[101],[102]. Routing topologies can be classified as either global or local knowledge. Global knowledge implies that the sender has complete visibility of all networked nodes, links, and capacities. In contrast, local knowledge

only provides information about the sender's immediate neighbours and their capacities [92]. The employment of specific routing algorithm techniques can lead to challenges in efficiency. These challenges may include depleting capacities, resulting in payment failures, potentially leaking sensitive information, and overlooking cheaper fee paths. As a result, enhancing routing remains a substantial open challenge for researchers and developers in the field [17], [27], [39].

5.3.6 REBALANCING

Exhausted channels are typically closed, refunded, and reopened following an on-chain lifecycle. However, opening and closing channels can lead to time and cost issues [104]. Rebalancing, essential to ensure optimal channel performance, is not inherently supported by the natural design of channels. As a result, achieving rebalancing is not a straightforward task, especially when dealing with many closed channels, leading to reduced channel availability, resulting in lower transaction success rates and ultimately impacting overall efficiency [92],[104]. Implementing balanced models, particularly in routing algorithms, remains a significant challenge and an open issue for researchers and developers [32],[105].

5.3.7 COLLATERAL LOCKING

Collateral refers to the current channel capacity in the PCN. The collateral is passively affected by the length of the payment path. Longer routing paths with higher fees result in longer locking times, which can deplete the channel capacity [70] and affect the channel's availability. Additionally, the residual amount left unused in the channel after the transaction can lead to inefficiencies in the network [31],[53].

5.3.8 COMPATIBILITY

Compatibility with Bitcoin is vital in evaluating the effectiveness of methods used in various systems. As Bitcoin sets the standard for blockchain projects, striving for compatibility ensures Interoperability and user acceptance. When assessing a method, it is crucial to consider its alignment with the underlying infrastructure of the LN and its compatibility with Bitcoin [42],[50].

5.3.9 INTEROPERABILITY

Interoperability in PCNs refers to the seamless integration and collaboration of different payment channels and systems, enabling users to conduct transactions across various channels without encountering obstacles. In the context of the LN, Interoperability means that network nodes can establish payment channels with other nodes, regardless of their specific implementation. This unrestricted connectivity allows users to transact with any participant on the network, regardless of their wallet or implementation. Interoperability is essential for the scalability and expansion of PCNs, as it eliminates entry barriers and simplifies user transactions among different types of channels or blockchain designs. However, achieving Interoperability relies on communication protocols among PCN nodes, which can be impacted by privacy and security measures. An unbalanced interoperable mechanism can severely impact efficiency [43].

5.3.10 CHANNEL BUILT TYPES

Channel building in the PCN is classified into script-based and scriptless script types. Script-based payment channel uses regular Bitcoin scripting language, offering simplicity, and allowing for flexibility in defining the conditions under which funds can be spent in building communication protocols such as HTLC; however, it is complex due to the flexibility of scripting languages and even lack smart contract adoption. Scriptless channel relies on complex cryptographic techniques like Digital Signatures (DS) and Zero-Knowledge Proofs (ZKP) to enhance privacy and security, introducing a higher cryptographic burden and decreasing overall efficiency.

6. PCN SINGLEHOP SOLUTIONS MECHANISMS

The underlying network structure influences the architecture of PCN solutions. Singlehop or Payment Channel Hub (PCH) utilizes a star network configuration with a centralized intermediate node connecting all channels. In contrast, PCN involves multiple connected (hubs). The analysis of literature in this section focuses on the previously addressed challenges, their impact on other factors, and the overall efficiency assessment. Heilman et al. [107] introduced TumbleBit, a unidirectional PCH that relies on an untrusted intermediary called Tumbler. TumbleBit's key aim is to prevent adversaries from linking payments between payers and payees, providing an unlinkable payment hub. The proposed solution is compatible with classic Bitcoin infrastructure. Meanwhile, Tairi et al. [108] have proposed Atomic Locks (A^2L) that enhance TumbleBit's Interoperability and efficiency while preserving routing anonymity to maintain

identities. Cryptographic primitives like homomorphic encryption and adapter signature are used to blind the puzzle and ensure that the corresponding solution differs between the puzzle sent and received by the hub. It enables transaction transfers without revealing the linkage between sender and receiver. Qin et al. [109] incorporated Blind Channel into BlindHub, a bidirectional PCH that prioritizes payment privacy. Both users agree on each channel update, but only one user can see how the channel funds are redistributed. Furthermore, Heilman et al. [110] introduced blind signature contracts, an anonymous payment method that employs smart contracts and blind signatures to establish unlinkability and balance security. The solution ensures anonymity through epoch-based techniques, enabling payments within epochs while preserving anonymity if the intermediary does not deny services.

Avarikioti et al. [96] have devised Brick. A singlehop PCN stays secure under asynchronous communication mode with a blockchain. It employs a neutral and rational wardens committee to resolve dispute conflicts, transforming dispute resolution from on-chain to off-chain instances and improving PCN efficiency. Conversely, Mavroudis et al. [111] have designed Snappy. It proposes fast, secure, and scalable off-chain transactions in PCNs. Practical collaterals are introduced to reduce payment latency, increase stability, and secure payment channels between parties. Ye et al. [112] enabled Garou instantaneous and updatable off-chain transactions without third-party trust. It separates sending and receiving funds for high concurrency, providing efficient and secure offchain payments. ObliHub, proposed by Wang et al. [113], uses oblivious puzzle transfer to achieve anonymity among parties. It hides transaction directions and prevents the hub from distinguishing the puzzle origin and destination. The proposed protocol establishes a transfer connection between the sender and hub, concealing the sender and receiver identities during the transfer. Additionally, RouTEE is a PCH Solution for transaction privacy and deposit reusability proposed by Lee et al. [114] to guarantee transaction privacy, deposit reusability, and blockchain interoperability. It introduces an atomic deposit protocol and privacy-preserving deposit certification to ensure fair payment channels and confidentiality of transaction values. Routing Fee Optimizing in PCN, suggested by Sali and Zohar [115], focuses on optimizing routing fees in PCNs to avoid the dominancy of certain financially capable parties. It employs spanning trees and game-theoretic models to achieve optimal liquidity and reduce costs.

Boros is another solution introduced by Zhang et al. [116] in which it builds a channel hub to connect multiple channels within a single controlling hub. It addresses the issue of channel depletion and large required deposits, enhancing liquidity in the network. WISER proposed by Tiwari et al. [117] meant to enable multiple hubs to collaborate using Multi-Party Computation (MPC) to aggregate transactions into a single monetary flow, providing optimal liquidity usage and efficient transaction aggregation meanwhile, privacy preserving route discovery by Pietrzak et al. [118] have designed LightPIR in which, it offers a privacy preserving route discovery mechanism for finding the shortest path within the PCN. It efficiently utilizes hub labelling algorithms and private information retrieval. Finally, Mirzaei et al. [119] introduced Garrison, a distributed PCH scheme with watchtower. It acts as a guardian watchtower in LN payment channels, providing high-level security monitoring. It incentivizes watchtowers to behave honestly while , protecting clients' channels against fraud attempts. PCH aims to reduce routing overhead and shorten paths; however, it comes with significant security, privacy, and efficiency trade-offs. Adopting a star topology introduces centralization in PCH, resulting in lower payment throughputs than decentralized topologies due to hubs' complete visual into participants' identities and payment histories [15], [120] therefore centralization is a real threat to efficiency. Consequently, heavy cryptographic techniques like blindization, ZKP, Non-Interactive Zero-Knowledge (NIZK), and DS becomes necessary to protect security and privacy which results on degraded efficiency due to low transaction success rates with higher consumed times. PCH Previously illustrated drawbacks remain an open challenge that requires further exploration and adequate solutions. Table 9 presents routing solutions conducted.

Table 9. - Singlehop Efficiency Factors Analysis.

Schema	Atomicity	Privacy		Balance Security	Dispute	Rebalancing	Routing	Channel Building Type		Interoperability	Fee Minimization	Collateral Locking Reduction	Compatibility
		VP	RA					Script	Script less				
[96]	√			√	Off				√	DS,H,TL			ETH
[97]	√			√	Off			√		HTLC			BTC
[100]	√	√	√	√	On					PSS,NIZK, PCS			BTC
[107]	√		√		On			√		HTLC			BTC
[108]	√		√		On				√	DS,TL			BTC
[109]	√		√	√	On				√	DS,TL			BTC
[110]	√			√	On				√	BS,TL			BTC
[111]	√			√	On				√	DS,TL	√	√	ETH
[112]	√			√	On				√	HTLC			ETH
[113]	√	√	√	√	On				√	DS,ZKP			BTC
[114]	√				On		√	√		SGX	√		BTC
[115]					On			√		HTLC	√	√	NS
[116]	√				On	√			√	DS,TL	√	√	ETH
[117]	√	√		√	On			√		HTLC	√	√	NS
[118]	√	√			On		√		√	Others	√		BTC
[119]	√	√		√	On				√	DS,TL			BTC
[121]	√				On			√		HTLC			BTC
[122]	√	√	√	√	On				√	DS,ZKP			BTC
[123]	√	√	√	√	On				√	DS,TL			BTC
[124]	√				On		√	√		HTLC	√		BTC
[125]	√			√	On			√		HTLC	√		BTC

Dispute (On/Off): Onchain/Offchain Mode**, HTLC:** Hash Time Locking Contract**, DS:** Digital Signature**, TL:** Time Locking**, BS:** Blind Signature**, ZKP:** Zero Knowledge Proof**, H:** Hash Function**, SGX:** Intel Chip**, PSS:** Pointcheval and Sanders Signature**, NIZK:** Non-Interactive Zero Knowledge Proof**, PCS:** Pederson Commitment Scheme**, NS:** Not Specified**, BTC:** Bitcoin**, ETH:** Ethereum**.**

7. PCN MULTIHOP SOLUTION MECHANISMS

Multihop PCNs operate in a decentralized and trustless environment through a linear networking model to establish payment paths with multiple hops between senders and receivers. This innovative approach addresses the efficiency challenges in PCN and effectively overcomes the limitations of singlehop solutions. Multihop PCNs have been designed to tackle various efficiency issues in the payment channel network ecosystem. Current analyzed solutions have been classified based on efficiency challenges discussed earlier.

7.1 ROUTING BASED SOLUTIONS

Malavolta et al. [94] introduced a routing algorithm based on the Breadth First Algorithm (BFS), Credit Network (CN), and centralized landmark, while Prihodoko et al. [126] proposed Flare, which comprises two stages: Proactive and Reactive. Proactive involves constructing a routing at each node, and Reactive finds a route from the sender to the receiver. Roos et al. [127] developed SpeedyMurmur using BFS, Voute, and greedy algorithms to find the shortest paths while considering available capacities. Yu et al. [88] designed CoinExpress, utilizing the distributed Ford-Fulkerson algorithm and a locking technique to handle concurrency in specific channels. Stasi et al. [74] proposed two schemes utilizing HTLC in multihop PCNs. The first scheme presented a novel approach for applying fees, and the second was a multipath routing payment method based on atomic payments. Conversely, Dong et al. [77] proposed Celer, which utilizes state channels and offchain computation to improve transaction throughput and reduce fees. Grunspan et al. [128] improved the scalability of PCNs with their ANT colony-inspired algorithm, aiming to find the most efficient path between nodes. Werman and Zohar [129] introduced a routing algorithm to avoid deadlocks by using channel reserves, dual-funded channels, and fee-based selection of payment channels. Wang et al. [130] proposed Flare with "elephant payments," a modified max-flow algorithm based on Edmond-Karp, to identify a set of k paths with sufficient capacity for routing large payments. For mice payments, a routing table is maintained at each node to identify the path to the receiver.

Zhang and Yang [103] introduced the CheaPay protocol to minimize fees for routing payments along a single path, comprising payment path construction and HTLC establishment to handle payment cancellations. Thakur and Breslin [131] presented the flocking algorithm within Path Based Transfer (PBT), enabling balanced channel networks without revealing specific channel balance information. Sivaraman et al. [132] aimed to provide efficient and scalable payment routing using a spider network topology and a set of routing algorithms to optimize payment routing. Mazumdar et al. [133] presented the Hushrely algorithm, leveraging residual amounts and introducing a new routing algorithm based on push-relabel and digital signatures to improve payment flow in PCNs. Bagaria et al. [134] introduced Boomerang, aiming to improve latency and throughput by duplicating payments across multiple channels. Eckey et al. [92] proposed a routing algorithm leveraging BFS, spanning trees, and Dijkstra's algorithm to split payments dynamically using local topology knowledge, leaving path selection to transferring nodes. Lin et al. [101] introduced FSTR, a payment network routing algorithm optimizing path selection for reduced funds skewness and increased transaction success probability. Xue et al. [102] proposed EPA-Route, utilizing a reputation system to encourage honest and efficient behaviour from payment channel operators, and an "energy-based model" to determine the most cost-effective routing path. Zhang and Yang [135] designed an efficient routing algorithm resistant to transaction failure while minimizing worst-case transaction fees. Rahimpour and Khabazian [136] suggested Spear routing, a redundant payment-based algorithm with low computational cost and less time lock.

Ersoy et al. [137] offered a re-routing solution to unlock coins held by intermediary parties in a multi-hop payment before its completion. Hong et al. [69] presented Auto-Tune routing, leveraging dynamic and implicit network views to automatically divide payments into optimal splitting amounts, maximizing the success probability. However, it is important to note that some of these proposed algorithms may not fully address security, privacy, conditional transfer, scalability, and dispute resolution concerns due to centralization or insufficient consideration in their design. Incompatibility issues and inefficiency in terms of computational resources, storage, communication, and time overhead may also be present. Further research and analysis are needed to address these challenges and develop more robust and efficient routing algorithms for multihop PCNs. Table 10 presents routing solutions conducted.

Table 10. - Routing Based Solutions Analysis.

Schema	Privacy		Atomicity	Balance Security	Dispute Mechanisms		WA	Routing	Rebalancing	Fee Optimization	Collateral Locking Period	Techniques & Methods	Advantages	Drawbacks	Compatibility		
	RA	VP			Off	On									LN	Bitcoin	Others
[31]			√	√		√		√		√		HTLC	Fast, RE	LRT, NRTF	√	√	
[69]			√	√		√		√				OOB	RE	LS	√	√	
[74]			√	√		√		√		√		HTLC	RE, Low TX fees	SWA	√	√	
[77]			√	√		√	√	√				StC, SdC	Fast, scalable	CNT, Trust is needed in CeN		√	√
[88]			√	√		√		√				FFA, DS	RE	CO	√	√	
[92]	√	√	√	√		√		√				SPN, DJK	RE	LP requires special hardware		√	
[94]								√				VSS, CN	First to split payments	CNT, CO		√	√
[101]			√	√		√		√		√		SAA	RE, fairness in payment routing	LPCN			√
[102]			√	√		√		√		√		HTLC, OR	High success rate and RE and secure	LPCN, may not work in low liquidity, High traffic network		√	
[103]			√	√	√	√		√			√	Multi-hop HTLC	Reduce fund locking time.	SWA	√	√	
[126]			√	√				√				ECDSA,SDG	RE	CO	√	√	
[127]	√	√									√	BFS, Vout e	RE	CO			√
[128]			√	√		√		√				HL, SDS	RE	LS	√	√	

[129]			√	√	√			√			AdhDDV	RE	LS		√		
[130]			√	√		√		√		√	MMF	RE	SWA	√	√		
[131]						√		√			FLA	Balanced Networks	LP&S	√	√		
[132]				√		√		√			MS, OR, SN	Efficient, Reduce TX fees	CO		√	√	
[133]			√	√		√	√	√			PRA, DS	Efficient payment flow problem in PCN is solved	CO	√	√		
[134]			√	√		√		√		√	HTLC, VSS	Increase Success ratio, Low latency	NRTF	√	√		
[135]		√	√	√	√	√		√			MPC	Robust against malicious actors, Efficient, Fast	LS, SWA	√	√		
[136]	√		√	√		√		√			H^2TLC	Fast & Efficient	LS, HR	√	√		
[138]			√	√		√		√			HTLC	RE	LPCN	√	√		

VSS: Verified secret sharing, **CN**: Credit network, **ECDSA:** Elliptic curve digital signature algorithm, **DG:** Digital signature, **SDS:** Schnorr digital signature, **AdhDDV:** Ad-hoc on Demand Distance Vector, **HTLC:** Hash time locking contracts, **HL:** Hash locking, **OOB:** Out of Band channels, **StC:** State channel, **SdC:** Sidechains, **MMF:** Modified max flow, **PRA:** Push relabel algorithm, **MHTLC:** Modified HTLC, **MS:** Multisignature, **OR:** Onion routing, **SN:** Spider network, **SPN:** Spanning tree, **DJK:** Dijkstra, **FFA:** Ford Fulkerson Algorithm, **BFS:** Breadth First Algorithm. **CO:** Complexity Overhead, **CNT:** Centralization, **LS:** Limited Scalability, **CeN:** Celer Network, **LP&S:** Lack of privacy and Security, **SWA:** Suspected to Wormhole Attack, **HR:** High Redundancy, **LPCN:** Limited to PCN, **LP:** Limited privacy, **FLA:** Flocking Algorithm, **LRT:** Limited Routing Topology, **NRTF:** Not resilient to Transaction Failure, **SAA:** Skewness Aware Algorithm, **RE:** Routing Efficiency, **TX:** Transaction, **LN:** Lightning Network.

7.2 REBALANCING BASED SOLUTIONS

Participants strive to overcome the challenges of channel depletion and inefficiency. Countless efforts have been made to design middle-ground solutions to reduce channel depletion, extend channel lifespan, and enhance overall network efficiency. This literary narrative delves into the remarkable proposals and inventive protocols that have emerged in this quest. Revive was proposed by Khalil and Gervais [33], a pioneering initiative to replenish exhausted channels within the network. The Revive protocol achieves efficient scaling while preventing depletion by skillfully relocating capacities and sidestepping regular rebalancing procedures. Meanwhile, Egger et al. [32] introduce a protocol leveraging Multiple Input and Multiple Output (MIMO) transactions and digital signatures as cryptographic foundations. This breakthrough enables synchronized off-chain updates for multiple payment channels, ensuring independent functionality while minimizing locked collateral, known as the Atomic Multi-Channel Update (AMCU). Zhong et al. [78] introduce the "Secure Large-scale Instant Payment" (SLIP) system, a marvel that enhances blockchain channel capacity. Through a seamless interconnection of off-chain channels using hash functions and aggregate signature schemes, tokens locked within these channels can freely circulate. Subramanian et al. [106] contribute to the rebalancing design by focusing on unidirectional mode, implementing acyclic payment networks where each node strategically rebalances channels through local metadata. Miller et al. [59] reveal their masterpiece, "Sprite," aiming to reduce collateral locking time, prolong

channel life, and bolster efficiency. The Global Preimage Manager (GPM) is central to their solution, a smart contract incentivizing path providers with routing fees, allowing channel funds to support others.

Ersoy et al. [93] presented an optimization solution using a heuristic algorithm based on the greedy approach. However, it prioritizes local optimization over global efficiency. Pickhardt and Nowostawski [139] usher in a new understanding of imbalanced networks, quantifying node imbalance using the Gini coefficient. PnP was designed by Li et al. [41], a channel balancing service incorporating epoch estimations to minimize overall channel deposits based on payment demands. Tikhomirov et al. [140] unveil their heuristic probing algorithm, accurately identifying proper channels within the LN. Meanwhile, Jourenko et al. [141] offer a solution to reduce collateral requirements through payment trees, effectively lowering transaction costs. Awathare et al. [142] propose "REBAL," which targets increased transaction success by addressing channel imbalances. It achieves this by selecting the most extended cycle involving each node for rebalancing and intelligent re-routing to prevent transaction rejections. Ge et al. [143] present Shaduf, an off-chain rebalancing scheme that tackles channel depletion by enabling unlimited off-chain coin transfers after an initial on-chain binding. Furthermore, they explore privacy enhancements through secure computation and ZKP while maintaining efficiency and non-cycle rebalancing. Ge et al. [144] improved privacy in payment channel rebalancing using secure computation and ZKP while maintaining efficiency and non-cycle rebalancing. Avarikioti et al. [145] pioneer a new rebalancing protocol that combines privacy and global optimality, maximizing received amounts per channel. Delegates are chosen, precise amounts calculated, and a linear program is employed to optimize total rebalanced funds. Wu and Jiang [105] propose a "Pooling" scheme where heavy-weighted nodes are connected with weaker subnodes, forming several clusters to strengthen channel liquidity.

Multiple supernodes manage each cluster, creating a network of interconnected supernodes within the LN. However, despite the ingenuity of these solutions, challenges remain open. Privacy, security, and conditional transfer have not been fully achieved in most cases, leaving some vulnerable to potential weaknesses. Compatibility with the Bitcoin infrastructure is another drawback that hampers progress. Additionally, some designs fall short in achieving their desired targets and preventing channel depletion, while disputes remain inadequately supported, resulting in overall inefficiencies. Table 11 provides a detailed overview of the various rebalancing algorithms, analysis in the LN.

Table 11. - Rebalancing Based Solutions Analysis.

Schema	Privacy		Atomicity	Balance Security	Dispute Mechanisms		WA	Routing	Rebalancing	Fee Optimization	Collateral Locking Period	Techniques & Methods	Advantages	Drawbacks	Compatibility		
	RA	VP			Off	On									LN	Bitcoin	Others
[32]			√	√		√						DS, MIMO	Channels function autonomously	CO, CNT	√	√	
[33]			√	√					√	√	√	DS+TL	Channel availability life extension	CO, INC			√
[41]			√			√					√	HTLC, PBFTS	Ensure balance availability	LP& S, SWA	√	√	
[59]		√	√	√		√						HTLC, GPM	Local dispute resolution,	CO			√
[78]						√	√	√	√			HL, AGS	Prevent DOS, Scalable to large networks	CO		√	√
[93]			√							√		GA	Increasing Node's profit	Non-CT	√	√	

[106]	√	√	√		√		√			NOA	Efficient rebalancing	LS	√	√
[105]		√	√				√			PA, HTLC, HE	Increase Liquidation	CO	√	√
[139]			√		√			√		SS, GC	Improved channel balance	CO, CM NR	√	√
[140]		√			√					PA	Discover fake channels	LS	√	√
[141]			√	√	√				√	PyT, RV, HTLC	Low collateral locking time	CO	√	√
[142]		√	√		√		√			CBA	Efficient, Fast	CO	√	√
[143]		√	√						√	HL, TL, AS	Efficient, secure rebalancing	INC		
[144]	√	√	√		√				√	ZKP, MPC, SC	Improved privacy	CO		
[145]	√	√	√		√		√		√	MPC, HTLC	Improved VP and BS for each rebalancing turn.	CNT, CO	√	√

RVC: Recursive virtual channel, **NOA:** Network optimization algorithm, **PBFT:** Path byzantine fault tolerance, **HL:** Hash Locks, **TL:** Time Locks, **AS:** Atomic Swap, **ZKP:** Zero-knowledge proof, **MPC:** Multiparty Computation, **SC:** Smart Contract, **PA:** Pooling Algorithm, **HE:** Homomorphic Encryption, **AGS:** Aggregate Signature, **DOS:** Denial of Service Attack, **PA:** Probing Algorithm, **GC:** Gini Coefficient, **SS:** Submarine Swap, **CO:** Complexity Overhead, **CNT:** Centralization, **LS:** Limited Scalability, **LP&S:** Lack of privacy and Security, **SWA:** Suspected to Wormhole Attack, **INC:** Incompatible, **GA:** Greedy Algorithm, **CBA:** Channel Balance Algorithm, **PyT:** Payment Tree.

7.3 DIVERSE SCALING SOLUTIONS

The rise of concepts such as virtuality and factories have been put forward, offering recursive channel production and hardwired devices to avoid intermediate hops, thereby increasing success rates. Decker and Russell [68] unveil "Eltoo," a revolutionary proposal simplifying payment channel management and reducing fraud risk by eliminating frequent blockchain updates. Instead, "update transactions" are broadcast only during disputes. Lowering transaction fees is achieved, too. Burchert et al.[25] introduce the "Channel Factory," where parties lock their coins into a shared deposit to create pairwise payment channels efficiently. Das et al. [146] present FastKitten, a framework for secure and efficient smart contract execution using Trusted Execution Environments (TEEs) without direct blockchain interaction. Jourenko et al. [147] introduce the "Lightweight Virtual Payment Channel," an off-chain protocol utilizing multisignatures and timelocks. Atomic setup and tear-down of new channels are enabled by splitting coins from existing ones, ensuring security and efficiency. Kiayias and Litos [148] propose the "Elmo" protocol, employing recursive virtual payment channels to facilitate faster micropayments by nesting multiple layers of payment channels using HTLCs. Addressing cross-chain transactions, Hoenisch et al. [149] present a cross-chain atomic swap protocol between Monero and Bitcoin chains, improving privacy and security through non-dependent relations between counterparties. Liao et al. [150] introduce "Speedster," supporting the creation and funding of off-chain accounts protected by TEEs. Multi-hop transfers using smart contracts ensure channel confidentiality, authenticity, finalization, and dispute resolution without on-chain interactions. Thyagarajan et al. [151] propose "Universal Atomic Swaps," offering a generic protocol for secure coin exchange across blockchains without custom scripting languages.

Finally, Dziembowski and Kedziar [152] delve into non-atomic payment splitting in channel networks with “EthNA”. This protocol allows the recursive splitting of payments into sub-payments, ensuring honest behaviour and a punishing mechanism without complex techniques like NIZK or homomorphic signature schemes. Despite the brilliance of these solutions, challenges persist. Computation, communication, and time overhead are substantial, raising concerns about

privacy and security, leaving some vulnerable to weaknesses. Compatibility remains a question, and disputes are not thoroughly addressed, resulting in reduced overall efficiency. Table 12 offers an in-depth analysis of diverse scaling solutions.

Table 12. - Diverse Scaling Solution Analysis.

Schema	Privacy		Atomicity	Balance Security	Dispute Mechanisms		WA	Routing	Rebalancing	Fee Optimization	Collateral Locking	Techniques & Methods	Advantages	Drawbacks	Compatibility		
	RA	VP			Off	On									LN	Bitcoin	Others
[25]			√			√						HTLC	Reduce storage communication overhead	Working entirely offchain	√	√	
[68]	√		√	√		√						HTLC, OR	Simpler, efficient.	L2P, not yet widely adopted, RRPAC		√	
[146]			√	√		√		√				DS,SC	Improving scalability, privacy	Limited to Bitcoin.		√	
[148]			√	√						√		SDS, RVC	Fast	L2P, RRPAC		√	
[149]			√	√		√						HTL, TDSA, PDC	Monero network.	CO, Incomplete privacy.		√	√
[150]			√	√		√						TEE, SC	Efficient multiparty state channel	Requires H/W enclave, Centrality, CO	√	√	
[151]	√	√	√	√		√						DSA, TL, SC	No centralized exchange, better security	CO			
[152]						√		√				VSC	-	Not proven yet, CO.			√
[153]			√	√	√					√		TL, MDS	Better routing and lower transaction fees.	CO.		√	

TDSA: Threshold Digital Signature, **PDC:** Pederson Commitment, **RVC:** Recursive Virtual channel, **TL:** Time Locks, **SC:** Smart Contract, **ADS:** Aggregated Digital Signature, **MDS:** Multiparty Digital Signature, **VSC:** Verifiable Secret Sharing, **OR:** Onion Routing, **CO:** Complexity Overhead, **L2P:** Limited to Two Parties, **RRPAC:** Require Routing Payment Active Channel.

7.4 PRIVACY AND SECURITY-BASED SOLUTIONS

Privacy and security are critical factors supporting efficiency in payment protocols. Breaching them can lead to undesired consequences, such as transaction success rate issues, long finalization times, and fund theft. Proposed solutions to protect privacy and security vary in their approaches, but some may not be compatible with the Bitcoin infrastructure or require heavy cryptographic techniques that impact efficiency. Zhang et al. [154] propose a protocol for atomic payment swaps in PCN, ensuring resilience to WA by combining onion routing, sidechains, and HTLCs. Grundmann et al. [155] present a secure ticketing system using adaptor signatures and HTLCs for efficient payment and ticket selling in public transportation. Kuwahara et al. [89] improve LN's privacy and security with Discreet Log Contracts (DLCs). Bentov et al. [156] introduce Tesseract, a real-time cryptocurrency exchange solution utilizing TEE for secure

peer-to-peer transactions. Lind et al. [120] propose Teechain, a payment network using TEE and committee chains for enhanced security. Liu et al. [157] present Generalized Multi-hop Locks (GMHL) with adaptor signatures and randomizable puzzles, offering atomicity, privacy, and generality in PCNs. Tripathy and Mohanty [75] designed Multi-hop Anonymous and Privacy Preserving PCN (MAPPCN) using elliptic curve group-based operations for better privacy performance against WA. Mohanty and Tripathy [73] propose Neo-HTLC and KTLC, two algorithms based on HTLC, where the first algorithm requires no setup phase; however, it remains incompatible with LN due to leveraging garlic routing, while KTLC has a setup phase and performs better efficiency. Both ensure secure, private, and consistent payment channels.

Yu et al. [87] introduced the Chameleon Hash Time Lock Contract (CHTLC), a modified algorithm inspired by [71]. It replaces the Fulgor hash concept with the more efficient and highly secure Chameleon hash function. CHTLC follows a single path routing within the LN, assuming full knowledge of the path and available capacities. It consists of three phases: setup, lock, and unlock, and it offers efficiency and security while preserving RA, VP, and BS . Yu et al. [158] proposed zk-PCN, a privacy-focused algorithm based on Yao's millionaire problem. It hides authentic balances and replaces them with fake public balances to achieve VP, RA, and BS. The protocol uses Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) a better version of ZKP and employs onion routing for anonymous communication among path participants. Platypus, introduced by Ranchala-Pedrosa and Garmoli [91], addresses scalability limitations in the Bitcoin network using a sidechain solution. It offers enhanced privacy and security without relying on synchrony or a trusted execution environment. Erdin et al. [76] designed a scalable private payment channel network with privacy guarantees, utilizing channel multiplexing and off-chain transaction aggregation for improved scalability and privacy. Malavolta et al. [71] proposed Multi-Hop HTLC, addressing privacy and concurrency issues in PCN using the Fulgor cryptographic technique. It involves contract creation release phases and handles concurrent payments efficiently. Moreover, Yu et al. [72] proposed an innovative solution to enhance the path probing-based routing algorithm, tackling the issue of anonymity through the application of hash (MAC) and symmetric encryption.

The essence of their work lies in introducing an anonymous path probing protocol, ensuring the preservation of anonymity for both senders and recipients. By integrating this protocol with privacy-preserving payment contracts, a comprehensive protocol stack for privacy preserving payments in PCN is formed. The core concept involves enabling each intermediate node to establish a symmetric key with the sender. This key then encrypts the queried data and includes essential information required for future decryption at the recipient's end, ensuring security during the path probing process. The Universal Re-encryption protocol is employed to re-encrypt the probe at each hop. The symmetric key derivation technique draws inspiration from established systems such as Sphinx and HORNET. Malavolta et al. [90] proposed Anonymous Multihop Locks (AMHL), a proof of concept for script-based and scriptless channels. AMHL utilizes a One-Way Homomorphic Hash function (OWHHF) in script channels ,Schnorr and ECDSA signature schemes in scriptless channels for locking and unlocking. The protocol achieves atomicity, VP, and reduced blockchain load. Mazumdar et al. [70] proposed leveraging multipath payments instead of single-path payments, addressing atomicity violation and time latency. They adopted a scriptless approach using ECDSA under the discrete logarithm problem to create their cryptographic commitment scheme. The security and privacy goals evaluated are RA, VP, CS, and atomicity. Each node is assumed to fully visualize neighbors, routes, and capacities. The payment channels are ordered using the BFS algorithm as a binary tree starting from receivers. Two paths, P1 and P2, are proposed, where nodes have knowledge of incoming and outgoing contracts. The protocol involves three phases: KeyGen Phase, Setup Phase, and Time Lock Contract Phases. The authors claim faster payments, reduced setup costs, and atomicity assurance, while leveraging core Bitcoin scripts and reducing space overhead.

Aumayr et al. [159] introduced Thora, which leverages multipath payments for atomicity and VP. It utilizes elliptic curve digital signatures and timelocks for cryptographic commitment. Osuntokun and Fromknecht [160] designed the Atomic Multi-Path (AMP) routing scheme for large payments through multiple channels. It splits payments and uses HTLC for atomicity, ensuring successful routing and payment privacy. Lin et al. [58] proposed a Distributed HTLC (D-HTLC) based smart contract that employs proactive and reactive routing. It addresses overloading and privacy issues but lacks efficiency, VP, and RA. Van Dam and Abdul Kadir [161] aimed to enhance LN privacy using differentially private payment channels, adding noise to payment amounts for improved privacy and security. However, there are several important considerations to address. Solutions are either fulfil security and privacy but at the cost of efficiency due to their reliance on heavy cryptographic techniques resulting in inefficient balancing complexities, centralization, and significant computational, storage, and communication concerns due to their reliance on heavy cryptographic techniques. or they could achieve better efficiency while remaining incompatible with LN Bitcoin. Furthermore, the variation among these solutions lies on their supports for privacy and security properties leading in some cases to violate conditional

transfer properties causing WA. Further investigations are required to overcome these limitations in order to must enhance the protocol's efficiency, privacy and security while ensuring it meets conditional transfer criteria through balanced solutions that combines lightweight methods and compatibility with LN. Table 13 illustrates the analysis conducted.

Table 13. - Privacy and Security Solutions Analysis.

Schema	Privacy		Atomicity	Balance Security	Dispute Mechanisms		WA	Routing	Fee Optimization	Rebalancing	Collateral Locking Period	Techniques & Methods	Advantages	Drawbacks	Compatibility		
	RA	VP			Off	On									LN	Bitcoin	Others
[58]		√	√	√	√			√				SC, D-HTLC	Local dispute resolution	CO		√	
[70]		√	√	√								ECDSA, HTLC	Dynamic, Reduce TX forwarding failure.	CO	√	√	
[71]	√		√	√		√	√					ZKP, HTLC	Solves privacy and supports Concurrent payment	SWA, PD, CO.	√	√	
[72]	√		√	√				√				SE, HMAC	Privacy approach to path probing	CO	√	√	
[73]	√	√	√	√		√	√					HTLC, GR	FE	INBTC			√
[73]	√	√	√	√		√	√					SE, OR	FE	SKE	√	√	
[75]	√	√	√	√		√	√					ECSM	FE	Proof of Concept	√	√	
[76]		√	√	√		√		√				BSG, ZKP	TX privacy, efficient	CO	√	√	
[87]	√	√	√	√		√	√					CHF, HTLC	FE	SKE	√	√	
[89]			√	√		√					√	DL, SC	Supports secure SC	Limited to LN, Non-scalable	√	√	
[90]	√		√	√		√	√					OWHHF, HE ECDSA, SDG	Solves WA	CO, INBTC	√	√	
[91]	√	√	√	√		√						NIZK, SC	Secure, Private Efficient,	CO			√
[120]			√	√				√				TEE, TSC	Enhances security by asynchronous access.	CO, CNT		√	
[154]			√	√	√		√					HTLC, SD	WA resilience	Low success rate, long finalizati on time	√	√	
[155]			√	√			√	√				SC	Generalizing PCN usage	CO			√

[156]			√	√			√			TEE, H	Realtime cross chain cryptocurrency exchange	CO	√	√	
[157]	√	√	√	√		√		√		ZKP, HL, DSA	Improved privacy and efficiency	CO	√	√	√
[158]	√	√	√	√		√				ZK-Snarks, ZKP	Secure	INBTC, CO			√
[159]		√	√			√			√	DS+TL	efficient collateral	CO		√	
[160]			√				√			HTLC	Conditional Transfer	Privacy, Security	√	√	
[161]	√	√	√	√		√		√		DPA	Improved privacy	Inaccurate TX amounts due to noise injection.	√	√	
[162]	√		√	√			√		√	TL, DS	Efficient single payment round	Support PBT, no support to HL models			√

SE: Symmetric Encryption, **HMAC**: Hash Machine Authentication Code, **SC:** Smart Contract, **NIZK:** Non-Interactive Zero-Knowledge, **PBFT:** Probabilistic Byzantine Fault Tolerance, **SA:** Sortation Algorithm, **BSG:** Blind Signature, **ZKP:** Zero Knowledge Proof, **TEE:** Trusted Execution Environment, **TSC:** Threshold Smart Contract, **PBT:** Path Based Transfer, **OWHHF:** One Way Homomorphic Hash Function, **ECDSA:** Elliptic Curve Digital Signature Algorithm, **SDG:** Schnorr Digital Signature, **GR:** Garlic Routing, **OR:** Onion Routing, **CHF:** Chameleon Hash Function, **ECSM:** Elliptic Curve Scalar Multiplication, **BTC:** Bitcoin, **D-HTLC:** Dynamic Hash Time Locking Contract, **SD:** Sidechain, **HE:** Homomorphic Encryption, **SKE:** Single Key Exposure, **CO:** Complexity Overhead, **SWA:** Suspected to Wormhole Attack, **CNT:** Centralization, **INBTC:** Incompatible with Bitcoin, **PD:** Payment Deadlock, **TX:** Transaction, **DPA:** Differential Privacy Approximation, **FE:** Fast and Efficient.

8. OPEN ISSUES AND FUTURE RESEARCH DIRECTIONS

- **Privacy & Security:** The impact of privacy and security on PCN efficiency is severe therefore future research must focus on finding crucial balance among compatibility and lightweight techniques in order to achieve balanced built cryptographic construction that is compatible with LN without compromising efficiency.

- **Routing:** Efficient and scalable routing algorithms are essential for PCN efficiency due to its responsibility on finding right path and capacities in which selected techniques to build these algorithms might fail payments. Future research could investigate new routing algorithms building techniques or combine other fields such as machine learning, AI, and others in order to optimize overall efficiency.

- **Dispute Resolution:** Dispute resolution mechanisms are critical for handling conflicts and ensuring fair PCN outcomes and due to its handling in on-chain it is fall under slow and costive blockchain lifecycle. Future research could focus on efficient local dispute handling within layer two while it must not conflict with compatibility and efficiency. Developing mechanisms for automated dispute resolution can also streamline the process and reduce manual intervention.

- **Rebalancing:** Effective channel rebalancing is crucial to maintain liquidity and avoid channel exhaustion and due to PCN nature that does not support rebalancing process while channels require to perform similar process of opening funding lifecycle within costive on-chain stage future research could explore automated and decentralized rebalancing strategies, utilizing newer techniques with aid of other techniques such AI that could be beneficial on balancing among channels usage in order to maintain balanced usage.

- **Collateral Locking:** Collateral locking is mainly affected by other factors such routing algorithms, privacy and security. Future research could investigate new collateral-locking approaches that minimize the locked funds while ensuring the network's security. Techniques like virtual collateral or offchain collateralization could be explored to reduce the impact on liquidity.

- **Fee Minimization:** Minimizing transaction fees is vital to encourage wider adoption of PCN specially for similar processes and users that cumulative costs can lead to exhaust their balances. Future research could focus on developing fee optimization algorithms that consider factors like network congestion, channel capacity, and transaction urgency assisted by other strategies and techniques such accumulation of several transactions for similar users in order to minimize network and financial resource usage. Implementation fee mechanisms could also help users optimize their transaction costs.

- **Interoperability:** Interoperability between different PCN is crucial for seamless cross-network transactions. Future research could explore standardization protocols and frameworks enabling interoperable payment channels across different networks, promoting a more connected and efficient payment ecosystem [163].

- **Compatibility:** Ensuring compatibility with Bitcoin, existing financial systems, and payment infrastructures is essential for adopting PCN. Future research could focus on developing interoperable bridges or gateway solutions that facilitate the integration of PCN with traditional financial systems, enabling a smooth transition towards decentralized payment solutions.

9. CONCLUSION

Blockchain technology is reshaping various industries including digital cryptocurrency, promising enhanced security, and a decentralized paradigm. However, scalability remains a challenge due to high validation times and transaction fees. Several scaling solutions have aimed to improve blockchain scalability. Layer one scaling solutions have attempted to address these issues but require extensive and costive substantial modifications to the blockchain core infrastructure resulting in compromised efficiency. Layer two scaling solutions, notably the LN with its payment channels and Payment Channels Network (PCN) have hugely improved blockchain scalability via removing transaction processing burden outside blockchain with inherited consensus and security leading to increased scalability and efficiency. Nonetheless, the implementation of PCN is not without its efficiency drawbacks. This study has conducted in depth investigation into the current efficiency impact factors in PCN wherein they have been identified and classified. Current challenges are also determined in terms of the trade-off among compatibility and techniques weights leveraged in the Existing solutions. Current solutions have been classified based on their building structure such singlehop and multihop showing their current achieved outcomes including limitations. Recent open issues and future research directions are also summarized to assist future researchers to further efficient PCN models. Future research directions should prioritize the development of well-balanced solutions that adeptly navigate the complexities of these influencing factors. This will pave the way for a more robust adoption and growth of PCNs, propelling blockchain technology toward its full transformative potential.

FUNDING:

Fundamental Research Grant Scheme (FRGS) of grant no. FRGS/1/2019/ICT03/USM/02/1. Postgraduate funding scheme (PFS) of grant no. PFS/9/2019/PhD 19166/01/Art College/Al-Iraqia University.

ACKNOWLEDGMENT:

The authors sincerely acknowledge and dedicate this paper to the support of the Ministry of Higher Education, Malaysia, and Universiti Sains Malaysia (USM). We would also like to express our deepest gratitude to the college of Art, Al-iraqia University, Baghdad, Iraq, for their highly appreciated sponsorship.

CONFLICTS OF INTEREST:

The authors declare no conflict of interest.

REFERENCES

[1] W. Baiod, J. Light, and A. Mahanti, "Blockchain Technology and its Applications Across Multiple Domains: A Survey," *J. Int. Technol. Inf. Manag.*, vol. 29, no. 4, pp. 78–119, Jan. 2021, doi: 10.58729/1941-6679.1482.

[2] M. Roy, M. Singh, and B. Radhakrishnan, "Blockchain Scalability: Solutions, Challenges and Future Possibilities," in *Proceedings of the 2nd International Conference on Signal and Data Processing*, K. P. Ray, A. Dixit, D. Adhikari, and R. Mathew, Eds., in Lecture Notes in Electrical Engineering. Singapore: Springer Nature, 2023, pp. 133–149. doi: 10.1007/978-981-99-1410-4_12.

[3] A. I. Sanka, M. Irfan, I. Huang, and R. C. C. Cheung, "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research," *Comput. Commun.*, vol. 169, pp. 179–201, Mar. 2021, doi: 10.1016/j.comcom.2020.12.028.

[4] T. Ye, M. Luo, Y. Yang, K.-K. R. Choo, and D. He, "A Survey on Redactable Blockchain: Challenges and Opportunities," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 3, pp. 1669–1683, May 2023, doi: 10.1109/TNSE.2022.3233448.

[5] M. Al-Abdullah, I. Alsmadi, R. AlAbdullah, and B. Farkas, "Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR," *Digit. Policy Regul. Gov.*, vol. 22, no. 5/6, pp. 389–411, Jan. 2020, doi: 10.1108/DPRG-04-2020-0050.

[6] R. Halim, "Decentralization, Scalability, and Security Trade-off in Blockchain System: Comparison on Different Approaches," Jul. 08, 2022. http://essay.utwente.nl/91994/ (accessed Jul. 03, 2023).

[7] N. Papadis and L. Tassiulas, "Blockchain-Based Payment Channel Networks: Challenges and Recent Advances," *IEEE Access*, vol. 8, pp. 227596–227609, 2020, doi: 10.1109/ACCESS.2020.3046020.

[8] Z. Wenhua, F. Qamar, T.-A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends," *Electronics*, vol. 12, no. 3, Art. no. 3, Jan. 2023, doi: 10.3390/electronics12030546.

[9] A. Hafid, A. S. Hafid, and M. Samih, "Scaling Blockchains: A Comprehensive Survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020, doi: 10.1109/ACCESS.2020.3007251.

[10] M. Platt *et al.*, "The energy footprint of blockchain consensus mechanisms beyond proof-of-work," in *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, IEEE, 2021, pp. 1135–1144.

[11] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no. 2, pp. 93–97, Jun. 2020, doi: 10.1016/j.icte.2019.08.001.

[12] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain Scaling Using Rollups: A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 93039–93054, 2022, doi: 10.1109/ACCESS.2022.3200051.

[13] G. Wang, Q. Wang, and S. Chen, "Exploring Blockchains Interoperability: A Systematic Survey," *ACM Comput. Surv.*, Feb. 2023, doi: 10.1145/3582882.

[14] J.Poon and second T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," *Lightening Network*, 2016. https://lightning.network/lightning-network-paper.pdf (accessed Oct. 01, 2022).

[15] D. Piatkivskyi and M. Nowostawski, "Split Payments in Payment Networks," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, J. Garcia-Alfaro, J. Herrera-Joancomartí, G. Livraga, and R. Rios, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, pp. 67–75. doi: 10.1007/978-3-030-00305-0_5.

[16] T.-V. Le and C.-L. Hsu, "A Systematic Literature Review of Blockchain Technology: Security Properties, Applications and Challenges," *J. Internet Technol.*, vol. 22, no. 4, Art. no. 4, Jul. 2021.

[17] L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais, "SoK: Layer-Two Blockchain Protocols," in *Financial Cryptography and Data Security*, J. Bonneau and N. Heninger, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 201–226. doi: 10.1007/978-3-030-51280-4_12.

[18] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic Literature Review of Challenges in Blockchain Scalability," *Appl. Sci.*, vol. 11, no. 20, Art. no. 20, Jan. 2021, doi: 10.3390/app11209372.

[19] C. Sguanci, R. Spatafora, and A. M. Vergani, "Layer 2 Blockchain Scaling: a Survey." arXiv, Jul. 22, 2021. doi: 10.48550/arXiv.2107.10881.

[20] S. Tikhomirov, P. Moreno-Sanchez, and M. Maffei, "A Quantitative Analysis of Security, Anonymity and Scalability for the Lightning Network," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Sep. 2020, pp. 387–396. doi: 10.1109/EuroSPW51379.2020.00059.

[21] M. Fazli, S. M. Nehzati, and M. Salarkia, "Building Stable Off-chain Payment Networks." arXiv, Jul. 07, 2021. doi: 10.48550/arXiv.2107.03367.

[22] C. Decker and R. Wattenhofer, "A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels," in *Stabilization, Safety, and Security of Distributed Systems*, A. Pelc and A. A. Schwarzmann, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2015, pp. 3–18. doi: 10.1007/978-3-319-21741-3_1.

[23] O. Ersoy, S. Roos, and Z. Erkin, "How to Profit from Payments Channels," in *Financial Cryptography and Data Security*, J. Bonneau and N. Heninger, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 284–303. doi: 10.1007/978-3-030-51280-4_16.

[24] S. Dziembowski, L. Eckey, S. Faust, and D. Malinowski, "Perun: Virtual Payment Hubs over Cryptocurrencies," in *2019 IEEE Symposium on Security and Privacy (SP)*, May 2019, pp. 106–123. doi: 10.1109/SP.2019.00020.

[25] C. Burchert, C. Decker, and R. Wattenhofer, "Scalable funding of Bitcoin micropayment channel networks," *R. Soc. Open Sci.*, vol. 5, no. 8, p. 180089, Aug. 2018, doi: 10.1098/rsos.180089.

[26] M. Jourenko, K. Kurazumi, M. Larangeira, and K. Tanaka, "SoK: A Taxonomy for Layer-2 Scalability Related Protocols for Cryptocurrencies." 2019. Accessed: Jul. 04, 2023. [Online]. Available: https://eprint.iacr.org/2019/352

[27] H. Qian, L. You, and A. Souri, "A Multipath Payment Scheme Supporting Proof of Payment," *Wirel. Commun. Mob. Comput.*, vol. 2022, Jan. 2022, doi: 10.1155/2022/9911915.

[28] S. Tochner, S. Schmid, and A. Zohar, "Hijacking Routes in Payment Channel Networks: A Predictability Tradeoff." arXiv, Sep. 15, 2019. doi: 10.48550/arXiv.1909.06890.

[29] A. Gangwal, H. R. Gangavalli, and A. Thirupathi, "A survey of Layer-two blockchain protocols," *J. Netw. Comput. Appl.*, vol. 209, p. 103539, Jan. 2023, doi: 10.1016/j.jnca.2022.103539.

[30] R. Gupta, N. K. Jadav, H. Mankodiya, M. D. Alshehri, S. Tanwar, and R. Sharma, "Blockchain and Onion-Routing-Based Secure Message Exchange System for Edge-Enabled IIoT," *IEEE Trans. Ind. Inform.*, vol. 19, no. 2, pp. 1965–1976, Feb. 2023, doi: 10.1109/TII.2022.3191444.

[31] Y. Zhang, D. Yang, and G. Xue, "CheaPay: An Optimal Algorithm for Fee Minimization in Blockchain-Based Payment Channel Networks," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, May 2019, pp. 1–6. doi: 10.1109/ICC.2019.8761804.

[32] C. Egger, P. Moreno-Sanchez, and M. Maffei, "Atomic Multi-Channel Updates with Constant Collateral in Bitcoin-Compatible Payment-Channel Networks." 2019. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2019/583

[33] R. Khalil and A. Gervais, "Revive: Rebalancing Off-Blockchain Payment Networks." 2017. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2017/823

[34] E. Erdin, M. Cebe, K. Akkaya, E. Bulut, and S. Uluagac, "A scalable private Bitcoin payment channel network with privacy guarantees," *J. Netw. Comput. Appl.*, vol. 180, p. 103021, Apr. 2021, doi: 10.1016/j.jnca.2021.103021.

[35] M. C. Kus Khalilov and A. Levi, "A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 3, pp. 2543–2585, 2018, doi: 10.1109/COMST.2018.2818623.

[36] R. Pickhardt, S. Tikhomirov, A. Biryukov, and M. Nowostawski, "Security and Privacy of Lightning Network Payments with Uncertain Channel Balances." arXiv, Mar. 15, 2021. doi: 10.48550/arXiv.2103.08576.

[37] Y. Huang, R. Li, J. Liu, Y. Xie, C. Zhang, and L. Wei, "A Privacy-Preserving Watchtower Scheme with Constant Storage Overhead," in *2022 IEEE/CIC International Conference on Communications in China (ICCC)*, Aug. 2022, pp. 737–742. doi: 10.1109/ICCC55456.2022.9880670.

[38] G. Kappos *et al.*, "An Empirical Analysis of Privacy in the Lightning Network," in *Financial Cryptography and Data Security*, N. Borisov and C. Diaz, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2021, pp. 167–186. doi: 10.1007/978-3-662-64322-8_8.

[39] A. M. Antonopoulos, O. Osuntokun, and R. Pickhardt, *Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments*. O'Reilly, 2022.

[40] S. P. Kumble, D. Epema, and S. Roos, "How Lightning's Routing Diminishes its Anonymity," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, in ARES 21. New York, NY, USA: Association for Computing Machinery, Aug. 2021, pp. 1–10. doi: 10.1145/3465481.3465761.

[41] P. Li, T. Miyazaki, and W. Zhou, "Secure Balance Planning of Off-blockchain Payment Channel Networks," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, Toronto, ON, Canada: IEEE Press, Jul. 2020, pp. 1728–1737. doi: 10.1109/INFOCOM41043.2020.9155375.

[42] E. Erdin, S. Mercan, and K. Akkaya, "An Evaluation of Cryptocurrency Payment Channel Networks and Their Privacy Implications." arXiv, Feb. 04, 2021. doi: 10.48550/arXiv.2102.02659.

[43] Y. Guo, M. Xu, D. Yu, Y. Yu, R. Ranjan, and X. Cheng, "Cross-Channel: Scalable Off-Chain Channels Supporting Fair and Atomic Cross-Chain Operations," *IEEE Trans. Comput.*, pp. 1–14, 2023, doi: 10.1109/TC.2023.3288765.

[44] S. S. Sahoo, M. M. Hosmane, and V. K. Chaurasiya, "A secure payment channel rebalancing model for layer-2 blockchain," *Internet Things*, vol. 22, p. 100822, Jul. 2023, doi: 10.1016/j.iot.2023.100822.

[45] Divya. K and M. Mohan, "Sidechain: A Scalable Blockchain," in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, May 2022, pp. 1337–1342. doi: 10.1109/ICAAIC53929.2022.9793041.

[46] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, 2022.

[47] A. S. Yadav, N. Singh, and D. S. Kushwaha, "Sidechain: storage land registry data using blockchain improve performance of search records," *Clust. Comput.*, vol. 25, no. 2, pp. 1475–1495, Apr. 2022, doi: 10.1007/s10586-022-03535-0.

[48] W. Ou, S. Huang, J. Zheng, Q. Zhang, G. Zeng, and W. Han, "An overview on cross-chain: Mechanism, platforms, challenges and advances," *Comput. Netw.*, vol. 218, p. 109378, Dec. 2022, doi: 10.1016/j.comnet.2022.109378.

[49] P. Han, Z. Yan, W. Ding, S. Fei, and Z. Wan, "A survey on cross-chain technologies," *Distrib. Ledger Technol. Res. Pract.*, vol. 2, no. 2, pp. 1–30, 2023.

[50] T. Xie *et al.*, "zkBridge: Trustless Cross-chain Bridges Made Practical," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, in CCS '22. New York, NY, USA: Association for Computing Machinery, Nov. 2022, pp. 3003–3017. doi: 10.1145/3548606.3560652.

[51] X. Jia, Z. Yu, J. Shao, R. Lu, G. Wei, and Z. Liu, "Cross-Chain Virtual Payment Channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 3401–3413, 2023, doi: 10.1109/TIFS.2023.3281064.

[52] L. Negka, A. Katsika, G. Spathoulas, and V. Plagianakos, "Blockchain state channels with compact states through the use of RSA accumulators," *Blockchain Res. Appl.*, vol. 4, no. 1, p. 100114, Mar. 2023, doi: 10.1016/j.bcra.2022.100114.

[53] A. Mirzaei, A. Sakzad, J. Yu, and R. Steinfeld, "FPPW: A Fair and Privacy Preserving Watchtower for Bitcoin," in *Financial Cryptography and Data Security*, N. Borisov and C. Diaz, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2021, pp. 151–169. doi: 10.1007/978-3-662-64331-0_8.

[54] K. N. Unnikrishnan and P. Victer Paul, "A Survey on Layer 2 Solutions to Achieve Scalability in Blockchain," in *Advances in Distributed Computing and Machine Learning*, R. R. Rout, S. K. Ghosh, P. K. Jana, A. K. Tripathy, J. P. Sahoo, and K.-C. Li, Eds., in Lecture Notes in Networks and Systems. Singapore: Springer Nature, 2022, pp. 205–216. doi: 10.1007/978-981-19-1018-0_18.

[55] M. Raikwar, D. Gligoroski, and K. Kralevska, "SoK of Used Cryptography in Blockchain," *IEEE Access*, vol. 7, pp. 148550–148575, 2019, doi: 10.1109/ACCESS.2019.2946983.

[56] P. McCorry, S. Bakshi, I. Bentov, S. Meiklejohn, and A. Miller, "Pisa: Arbitration Outsourcing for State Channels," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, in AFT '19. New York, NY, USA: Association for Computing Machinery, Oct. 2019, pp. 16–30. doi: 10.1145/3318041.3355461.

[57] S. Kim, Y. Kwon, and S. Cho, "A Survey of Scalability Solutions on Blockchain," in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct. 2018, pp. 1204–1207. doi: 10.1109/ICTC.2018.8539529.

[58] C. Lin, N. Ma, X. Wang, and J. Chen, "Rapido: Scaling blockchain with multi-path payment channels," *Neurocomputing*, vol. 406, pp. 322–332, Sep. 2020, doi: 10.1016/j.neucom.2019.09.114.

[59] A. Miller, I. Bentov, S. Bakshi, R. Kumaresan, and P. McCorry, "Sprites and State Channels: Payment Networks that Go Faster Than Lightning," in *Financial Cryptography and Data Security*, I. Goldberg and T. Moore, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019, pp. 508–526. doi: 10.1007/978-3-030-32101-7_30.

[60] P. McCorry, C. Buckland, S. Bakshi, K. Wüst, and A. Miller, "You sank my battleship! a case study to evaluate state channels as a scaling solution for cryptocurrencies," in *Financial Cryptography and Data Security: FC 2019 International Workshops, VOTING and WTSC, St. Kitts, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23*, Springer, 2020, pp. 35–49.

[61] L. D. Negka and G. P. Spathoulas, "Blockchain State Channels: A State of the Art," *IEEE Access*, vol. 9, pp. 160277–160298, 2021, doi: 10.1109/ACCESS.2021.3131419.

[62] Z. Avarikioti, O. S. Thyfronitis Litos, and R. Wattenhofer, "Cerberus channels: Incentivizing watchtowers for bitcoin," in *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24*, Springer, 2020, pp. 346–366.

[63] M. Du, P. Yang, W. Tian, and Z. Han, "Anti-Collusion Multiparty Smart Contracts for Distributed Watchtowers in Payment Channel Networks," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3600–3614, Dec. 2022, doi: 10.1109/JSAC.2022.3213355.

[64] A. Mirzaei, "Daric: A Storage Efficient Payment Channel With Penalization Mechanism," in *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, Jun. 2022, pp. 51–52. doi: 10.1109/DSN-S54099.2022.00029.

[65] R. Pass and abhi shelat, "Micropayments for Decentralized Currencies," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, in CCS '15. New York, NY, USA: Association for Computing Machinery, Oct. 2015, pp. 207–218. doi: 10.1145/2810103.2813713.

[66] J. Spilman, "[Bitcoin-development] Anti DoS for tx replacement," Apr. 20, 2013. Accessed: Jul. 18, 2023. [Online]. Available: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-April/002433.html

[67] C. Decker and R. Wattenhofer, "A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels," in *Stabilization, Safety, and Security of Distributed Systems*, A. Pelc and A. A. Schwarzmann, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2015, pp. 3–18. doi: 10.1007/978-3-319-21741-3_1.

[68] C. Decker and R. Russell, "eltoo : A Simple Layer 2 Protocol for Bitcoin," 2018. Accessed: Jul. 03, 2023. [Online]. Available: https://www.semanticscholar.org/paper/eltoo-%3A-A-Simple-Layer-2-Protocol-for-Bitcoin-Decker-Russell/afc2e810be32e0c0b20c277fa0c2774d3ec82ac7

[69] H.-J. Hong, S.-Y. Chang, and X. Zhou, "Auto-tune: An efficient autonomous multi-path payment routing algorithm for Payment Channel Networks," *Comput. Netw.*, vol. 225, p. 109659, Apr. 2023, doi: 10.1016/j.comnet.2023.109659.

[70] S. Mazumdar and S. Ruj, *CryptoMaze: Atomic Off-Chain Payments in Payment Channel Network*. 2020.

[71] G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei, and S. Ravi, "Concurrency and Privacy with Payment-Channel Networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, in CCS '17. New York, NY, USA: Association for Computing Machinery, Oct. 2017, pp. 455–471. doi: 10.1145/3133956.3134096.

[72] R. Yu, Y. Wan, V. T. Kilari, G. Xue, J. Tang, and D. Yang, "P4PCN: Privacy-preserving path probing for payment channel networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, IEEE, 2019, pp. 1–6.

[73] S. K. Mohanty and S. Tripathy, "n-HTLC: Neo hashed time-Lock commitment to defend against wormhole attack in payment channel networks," *Comput. Secur.*, vol. 106, p. 102291, Jul. 2021, doi: 10.1016/j.cose.2021.102291.

[74] G. D. Stasi, S. Avallone, R. Canonico, and G. Ventre, "Routing Payments on the Lightning Network," presented at the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE Computer Society, Jul. 2018, pp. 1161–1170. doi: 10.1109/Cybermatics_2018.2018.00209.

[75] S. Tripathy and S. K. Mohanty, "MAPPCN: Multi-hop Anonymous and Privacy-Preserving Payment Channel Network," in *Financial Cryptography and Data Security*, M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, and M. Sala, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 481–495. doi: 10.1007/978-3-030-54455-3_34.

[76] E. Erdin, M. Cebe, K. Akkaya, E. Bulut, and S. Uluagac, "A scalable private Bitcoin payment channel network with privacy guarantees," *J. Netw. Comput. Appl.*, vol. 180, p. 103021, Apr. 2021, doi: 10.1016/j.jnca.2021.103021.

[77] M. Dong, Q. Liang, X. Li, and J. Liu, "Celer Network: Bring Internet Scale to Every Blockchain." arXiv, Sep. 28, 2018. doi: 10.48550/arXiv.1810.00037.

[78] L. Zhong, Q. Wu, J. Xie, Z. Guan, and B. Qin, "A secure large-scale instant payment system based on blockchain," *Comput. Secur.*, vol. 84, pp. 349–364, Jul. 2019, doi: 10.1016/j.cose.2019.04.007.

[79] M. Liu and M. H. Au, "Practical Anonymous Multi-hop Locks for Lightning Network Compatible Payment Channel Networks," in *Network and System Security*, X. Yuan, G. Bai, C. Alcaraz, and S. Majumdar, Eds., in Lecture Notes in Computer Science. Cham: Springer Nature Switzerland, 2022, pp. 547–560. doi: 10.1007/978-3-031-23020-2_31.

[80] Y. Liu, Y. Wu, F. Zhao, and Y. Ren, "Balanced Off-Chain Payment Channel Network Routing Strategy Based On Weight Calculation," *Comput. J.*, p. bxad029, Apr. 2023, doi: 10.1093/comjnl/bxad029.

[81] S. Mazumdar, "Secure Off-chain Transactions in Blockchain-based Payment Channel Networks," Thesis, Indian Statistical Institute, Kolkata, 2022. Accessed: Jul. 05, 2023. [Online]. Available: http://localhost:8080/xmlui/handle/10263/7350

[82] O. Ali, M. Ally, Clutterbuck, and Y. Dwivedi, "The state of play of blockchain technology in the financial services sector: A systematic literature review," *Int. J. Inf. Manag.*, vol. 54, p. 102199, Oct. 2020, doi: 10.1016/j.ijinfomgt.2020.102199.

[83] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019, doi: 10.1016/j.jnca.2018.10.020.

[84] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digit. Commun. Netw.*, vol. 7, no. 3, pp. 295–307, Aug. 2021, doi: 10.1016/j.dcan.2020.05.008.

[85] Z. Lu, R. Han, and J. Yu, "General Congestion Attack on HTLC-Based Payment Channel Networks." 2020. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2020/456

[86] B. Weintraub, C. Nita-Rotaru, and S. Roos, "Structural Attacks on Local Routing in Payment Channel Networks," presented at the 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE Computer Society, Sep. 2021, pp. 367–379. doi: 10.1109/EuroSPW54576.2021.00046.

[87] B. Yu, S. K. Kermanshahi, A. Sakzad, and S. Nepal, "Chameleon Hash Time-Lock Contract for Privacy Preserving Payment Channel Networks," in *Provable Security*, R. Steinfeld and T. H. Yuen, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019, pp. 303–318. doi: 10.1007/978-3-030-31919-9_18.

[88] R. Yu, G. Xue, V. T. Kilari, D. Yang, and J. Tang, "CoinExpress: A Fast Payment Routing Mechanism in Blockchain-Based Payment Channel Networks," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, Jul. 2018, pp. 1–9. doi: 10.1109/ICCCN.2018.8487351.

[89] I. Kuwahara, "Discreet Log Contracts Channels and Integration in the Lightning Network," 2020. Accessed: Jul. 03, 2023. [Online]. Available: https://www.semanticscholar.org/paper/Discreet-Log-Contracts-Channels-and-Integration-in-Kuwahara/519db2a084ac4810ef194b12d144d642074db7f9

[90] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, "Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability." 2018. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2018/472

[91] A. Ranchal-Pedrosa and V. Gramoli, "Platypus: Offchain Protocol Without Synchrony," in *2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)*, Sep. 2019, pp. 1–8. doi: 10.1109/NCA.2019.8935037.

[92] L. Eckey, S. Faust, K. Hostáková, and S. Roos, "Splitting Payments Locally While Routing Interdimensionally." 2020. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2020/555

[93] O. Ersoy, S. Roos, and Z. Erkin, "How to Profit from Payments Channels," in *Financial Cryptography and Data Security*, J. Bonneau and N. Heninger, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 284–303. doi: 10.1007/978-3-030-51280-4_16.

[94] G. Malavolta, P. Moreno-Sanchez, A. Kate, and M. Maffei, "SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks." 2016. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2016/1054

[95] R. A. Haraty, M. Assi, and I. Rahal, *A Systematic Review of Anonymous Communication Systems*. SCITEPRESS, 2017. Accessed: Jul. 05, 2023. [Online]. Available: https://laur.lau.edu.lb:8443/xmlui/handle/10725/7122

[96] Z. Avarikioti, E. Kokoris-Kogias, R. Wattenhofer, and D. Zindros, "Brick: Asynchronous Incentive-Compatible Payment Channels," in *Financial Cryptography and Data Security*, N. Borisov and C. Diaz, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2021, pp. 209–230. doi: 10.1007/978-3-662-64331-0_11.

[97] Z. Avarikioti, O. S. Thyfronitis Litos, and R. Wattenhofer, "Cerberus Channels: Incentivizing Watchtowers for Bitcoin," in *Financial Cryptography and Data Security*, J. Bonneau and N. Heninger, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 346–366. doi: 10.1007/978-3-030-51280-4_19.

[98] J. Harris and A. Zohar, "Flood & Loot: A Systemic Attack on The Lightning Network," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, in AFT '20. New York, NY, USA: Association for Computing Machinery, Oct. 2020, pp. 202–213. doi: 10.1145/3419614.3423248.

[99] S. Mercan, E. Erdin, and K. Akkaya, "Improving transaction success rate in cryptocurrency payment channel networks," *Comput. Commun.*, vol. 166, pp. 196–207, Jan. 2021, doi: 10.1016/j.comcom.2020.12.009.

[100] Y. Li *et al.*, "PRI: PCH-based privacy-preserving with reusability and interoperability for enhancing blockchain scalability," *J. Parallel Distrib. Comput.*, vol. 180, p. 104721, Oct. 2023, doi: 10.1016/j.jpdc.2023.104721.

[101] S. Lin, J. Zhang, and W. Wu, "FSTR: Funds Skewness Aware Transaction Routing for Payment Channel Networks," in *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Jun. 2020, pp. 464–475. doi: 10.1109/DSN48063.2020.00060.

[102] H. Xue, Q. Huang, and Y. Bao, "EPA-Route: Routing payment channel network with high success rate and low payment fees," in *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*, IEEE, 2021, pp. 227–237.

[103] Y. Zhang and D. Yang, "RobustPay: Robust Payment Routing Protocol in Blockchain-based Payment Channel Networks," presented at the 2019 IEEE 27th International Conference on Network Protocols (ICNP), IEEE Computer Society, Oct. 2019, pp. 1–4. doi: 10.1109/ICNP.2019.8888094.

[104] Z. Hong, S. Guo, R. Zhang, P. Li, Y. Zhan, and W. Chen, "Cycle: Sustainable Off-Chain Payment Channel Network with Asynchronous Rebalancing," in *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Jun. 2022, pp. 41–53. doi: 10.1109/DSN53405.2022.00017.

[105] J. Wu and S. Jiang, "On increasing scalability and liquidation of lightning networks for blockchains," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2589–2600, 2022.

[106] L. M. Subramanian, G. Eswaraiah, and R. Vishwanathan, "Rebalancing in Acyclic Payment Networks," presented at the 2019 17th International Conference on Privacy, Security and Trust (PST), IEEE Computer Society, Aug. 2019, pp. 1–5. doi: 10.1109/PST47121.2019.8949051.

[107] E. Heilman, L. AlShenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "TumbleBit: an untrusted Bitcoin-compatible anonymous payment hub," 2017, doi: 10.14722/NDSS.2017.23086.

[108] E. Tairi, P. Moreno-Sanchez, and M. Maffei, "A2L: Anonymous Atomic Locks for Scalability in Payment Channel Hubs," in *2021 IEEE Symposium on Security and Privacy (SP)*, May 2021, pp. 1834–1851. doi: 10.1109/SP40001.2021.00111.

[109] X. Qin *et al.*, "BlindHub: Bitcoin-Compatible Privacy-Preserving Payment Channel Hubs Supporting Variable Amounts," presented at the 2023 IEEE Symposium on Security and Privacy (SP), IEEE Computer Society, Dec. 2022, pp. 2462–2480. doi: 10.1109/SP46215.2023.00116.

[110] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions," in *Financial Cryptography and Data Security*, J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2016, pp. 43–60. doi: 10.1007/978-3-662-53357-4_4.

[111] V. Mavroudis, K. Wüst, A. Dhar, K. Kostiainen, and S. Capkun, "Snappy: Fast On-chain Payments with Practical Collaterals." arXiv, Jan. 05, 2020. doi: 10.48550/arXiv.2001.01278.

[112] Y. Ye, Z. Ren, X. Luo, J. Zhang, and W. Wu, "Garou: An Efficient and Secure Off-Blockchain Multi-Party Payment Hub," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 4, pp. 4450–4461, Dec. 2021, doi: 10.1109/TNSM.2021.3101808.

[113] Y. Wang *et al.*, "Enabling scalable and unlinkable payment channel hubs with oblivious puzzle transfer," *Inf. Sci.*, vol. 630, pp. 713–726, Jun. 2023, doi: 10.1016/j.ins.2023.02.024.

[114] J. Lee, S. Kim, S. Park, and S.-M. Moon, "RouTEE: A Secure Payment Network Routing Hub using Trusted Execution Environments." arXiv, Dec. 08, 2020. doi: 10.48550/arXiv.2012.04254.

[115] Y. Sali and A. Zohar, "Optimizing Off-Chain Payment Networks in Cryptocurrencies." arXiv, Jul. 26, 2020. doi: 10.48550/arXiv.2007.09410.

[116] J. Zhang, Y. Ye, W. Wu, and X. Luo, "Boros: Secure and Efficient Off-Blockchain Transactions via Payment Channel Hub," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 1, pp. 407–421, Jan. 2023, doi: 10.1109/TDSC.2021.3135076.

[117] S. Tiwari, M. Yeo, Z. Avarikioti, I. Salem, K. Pietrzak, and S. Schmid, "Wiser: Increasing Throughput in Payment Channel Networks with Transaction Aggregation." arXiv, May 23, 2022. doi: 10.48550/arXiv.2205.11597.

[118] K. Pietrzak, I. Salem, S. Schmid, and M. Yeo, "LightPIR: Privacy-Preserving Route Discovery for Payment Channel Networks," in *2021 IFIP Networking Conference (IFIP Networking)*, Jun. 2021, pp. 1–9. doi: 10.23919/IFIPNetworking52078.2021.9472205.

[119] A. Mirzaei, A. Sakzad, J. Yu, and R. Steinfeld, "Garrison: A Novel Watchtower Scheme for Bitcoin." 2022. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2022/1300

[120] J. Lind, O. Naor, I. Eyal, F. Kelbert, E. G. Sirer, and P. Pietzuch, "Teechain: a secure payment network with asynchronous blockchain access," in *Proceedings of the 27th ACM Symposium on Operating Systems Principles*, in SOSP '19. New York, NY, USA: Association for Computing Machinery, Oct. 2019, pp. 63–79. doi: 10.1145/3341301.3359627.

[121] T. Mitani and A. Otsuka, "Anonymous probabilistic payment in payment hub." 2020. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2020/748

[122] M. Green and I. Miers, "Bolt: Anonymous Payment Channels for Decentralized Currencies," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, in CCS '17. New York, NY, USA: Association for Computing Machinery, Oct. 2017, pp. 473–489. doi: 10.1145/3133956.3134093.

[123] D. Zhang, J. Le, N. Mu, and X. Liao, "An Anonymous Off-Blockchain Micropayments Scheme for Cryptocurrencies in the Real World," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 50, no. 1, pp. 32–42, Jan. 2020, doi: 10.1109/TSMC.2018.2884289.

[124] Y. Van Engelshoven and S. Roos, "The Merchant: Avoiding Payment Channel Depletion through Incentives," in *2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, Aug. 2021, pp. 59–68. doi: 10.1109/DAPPS52256.2021.00012.

[125] M. Khabbazian, T. Nadahalli, and R. Wattenhofer, "Outpost: A Responsive Lightweight Watchtower," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, in AFT '19. New York, NY, USA: Association for Computing Machinery, Oct. 2019, pp. 31–40. doi: 10.1145/3318041.3355464.

[126] P. Prihodko, S. Zhigulin, M. Sahno, A. Ostrovskiy, and O. Osuntokun, "Flare : An Approach to Routing in Lightning Network White Paper," 2016. Accessed: Jul. 03, 2023. [Online]. Available: https://www.semanticscholar.org/paper/Flare-%3A-An-Approach-to-Routing-in-Lightning-Network-Prihodko-Zhigulin/4392166a1194010c844ec915694fd5c56da94301

[127] S. Roos, P. Moreno-Sanchez, A. Kate, and I. Goldberg, "Settling Payments Fast and Private: Efficient Decentralized Routing for Path-Based Transactions." arXiv, Dec. 13, 2017. doi: 10.48550/arXiv.1709.05748.

[128] C. Grunspan, G. Lehéricy, and R. Pérez-Marco, "Ant Routing scalability for the Lightning Network." arXiv, Feb. 04, 2020. doi: 10.48550/arXiv.2002.01374.

[129] S. Werman and A. Zohar, "Avoiding Deadlocks in Payment Channel Networks," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, J. Garcia-Alfaro, J. Herrera-Joancomartí, G. Livraga, and R. Rios, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, pp. 175–187. doi: 10.1007/978-3-030-00305-0_13.

[130] P. Wang, H. Xu, X. Jin, and T. Wang, "Flash: efficient dynamic routing for offchain networks," in *Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies*, in CoNEXT '19. New York, NY, USA: Association for Computing Machinery, Dec. 2019, pp. 370–381. doi: 10.1145/3359989.3365411.

[131] S. Thakur and J. G. Breslin, "A Balanced Routing Algorithm for Blockchain Offline Channels Using Flocking," in *Blockchain and Applications*, J. Prieto, A. K. Das, S. Ferretti, A. Pinto, and J. M. Corchado, Eds., in Advances in Intelligent Systems and Computing. Cham: Springer International Publishing, 2020, pp. 79–86. doi: 10.1007/978-3-030-23813-1_10.

[132] V. Sivaraman *et al.*, "High Throughput Cryptocurrency Routing in Payment Channel Networks," presented at the 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20), 2020, pp. 777–796. Accessed: Jul. 03, 2023. [Online]. Available: https://www.usenix.org/conference/nsdi20/presentation/sivaraman

[133] S. Mazumdar, S. Ruj, R. G. Singh, and A. Pal, "HushRelay: A privacy-preserving, efficient, and scalable routing algorithm for off-chain payments," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, 2020, pp. 1–5.

[134] V. Bagaria, J. Neu, and D. Tse, "Boomerang: Redundancy Improves Latency and Throughput in Payment-Channel Networks," 2020, pp. 304–324. doi: 10.1007/978-3-030-51280-4_17.

[135] Y. Zhang and D. Yang, "RobustPay+: Robust Payment Routing With Approximation Guarantee in Blockchain-Based Payment Channel Networks," *IEEEACM Trans. Netw.*, vol. 29, no. 04, pp. 1676–1686, Jul. 2021, doi: 10.1109/TNET.2021.3069725.

[136] S. Rahimpour and M. Khabbazian, "Spear: fast multi-path payment with redundancy," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, in AFT '21. New York, NY, USA: Association for Computing Machinery, Nov. 2021, pp. 183–191. doi: 10.1145/3479722.3480997.

[137] O. Ersoy, P. Moreno-Sanchez, and S. Roos, "Get Me out of This Payment! Bailout: An HTLC Re-routing Protocol." 2022. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2022/958

[138] O. Ersoy, P. Moreno-Sanchez, and S. Roos, "Get Me out of This Payment! Bailout: An HTLC Re-routing Protocol." 2022. Accessed: Jul. 06, 2023. [Online]. Available: https://eprint.iacr.org/2022/958

[139] R. Pickhardt and M. Nowostawski, "Imbalance measure and proactive channel rebalancing algorithm for the Lightning Network," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, May 2020, pp. 1–5. doi: 10.1109/ICBC48266.2020.9169456.

[140] S. Tikhomirov, R. Pickhardt, A. Biryukov, and M. Nowostawski, "Probing Channel Balances in the Lightning Network." arXiv, Apr. 01, 2020. doi: 10.48550/arXiv.2004.00333.

[141] M. Jourenko, M. Larangeira, and K. Tanaka, "Payment Trees: Low Collateral Payments for Payment Channel Networks," in *Financial Cryptography and Data Security*, N. Borisov and C. Diaz, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2021, pp. 189–208. doi: 10.1007/978-3-662-64331-0_10.

[142] N. Awathare, Suraj, Akash, V. J. Ribeiro, and U. Bellur, "REBAL: Channel Balancing for Payment Channel Networks," in *2021 29th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Nov. 2021, pp. 1–8. doi: 10.1109/MASCOTS53633.2021.9614304.

[143] Z. Ge, Y. Zhang, Y. Long, and D. Gu, "Shaduf: Non-Cycle Payment Channel Rebalancing," *Proc. 2022 Netw. Distrib. Syst. Secur. Symp.*, 2022, doi: 10.14722/ndss.2022.24203.

[144] Z. Ge, Y. Zhang, Y. Long, and D. Gu, "Shaduf++: Non-Cycle and Privacy-Preserving Payment Channel Rebalancing." 2022. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2022/388

[145] Z. Avarikioti, K. Pietrzak, I. Salem, S. Schmid, S. Tiwari, and M. Yeo, "Hide & Seek: Privacy-Preserving Rebalancing on Payment Channel Networks," in *Financial Cryptography and Data Security*, I. Eyal and J. Garay, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2022, pp. 358–373. doi: 10.1007/978-3-031-18283-9_17.

[146] P. Das *et al.*, "FASTKITTEN: practical smart contracts on bitcoin," in *Proceedings of the 28th USENIX Conference on Security Symposium*, in SEC'19. USA: USENIX Association, Aug. 2019, pp. 801–818.

[147] M. Jourenko, M. Larangeira, and K. Tanaka, "Lightweight Virtual Payment Channels," in *Cryptology and Network Security*, S. Krenn, H. Shulman, and S. Vaudenay, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 365–384. doi: 10.1007/978-3-030-65411-5_18.

[148] A. Kiayias and O. S. T. Litos, "Elmo: Recursive Virtual Payment Channels for Bitcoin." 2021. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2021/747

[149] P. Hoenisch, S. Mazumdar, P. Moreno-Sanchez, and S. Ruj, "LightSwap: An Atomic Swap Does Not Require Timeouts At Both Blockchains." 2022. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2022/1650

[150] J. Liao, F. Zhang, W. Sun, and W. Shi, "Speedster: An Efficient Multi-party State Channel via Enclaves," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, in ASIA CCS '22. New York, NY, USA: Association for Computing Machinery, May 2022, pp. 637–651. doi: 10.1145/3488932.3523259.

[151] S. A. Thyagarajan, G. Malavolta, and P. Moreno-Sánchez, "Universal Atomic Swaps: Secure Exchange of Coins Across All Blockchains." 2021. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2021/1612

[152] S. Dziembowski and P. Kędzior, "Non Atomic Payment Splitting in Channel Networks." 2020. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2020/166

[153] M. Jourenko, M. Larangeira, and K. Tanaka, "Lightweight Virtual Payment Channels," in *Cryptology and Network Security*, S. Krenn, H. Shulman, and S. Vaudenay, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 365–384. doi: 10.1007/978-3-030-65411-5_18.

[154] Q. Zhang, S. Cao, Y. Ni, T. Chen, and X. Zhang, "Enabling Privacy-Preserving Off-chain Payment via Hybrid Multi-hop Mechanism," in *ICC 2022 - IEEE International Conference on Communications*, May 2022, pp. 13–18. doi: 10.1109/ICC45855.2022.9839015.

[155] M. Grundmann, O. von Zastrow-Marcks, and H. Hartenstein, "On the Applicability of Payment Channel Networks for Allocation of Transport Ticket Revenues," in *2022 International Conference on Computer Communications and Networks (ICCCN)*, Jul. 2022, pp. 1–7. doi: 10.1109/ICCCN54977.2022.9868881.

[156] I. Bentov, Y. Ji, F. Zhang, L. Breidenbach, P. Daian, and A. Juels, "Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, in CCS '19. New York, NY, USA: Association for Computing Machinery, Nov. 2019, pp. 1521–1538. doi: 10.1145/3319535.3363221.

[157] Z. Liu, A. Yang, J. Weng, T. Li, H. Zeng, and X. Liang, "GMHL: Generalized Multi-Hop Locks for Privacy-Preserving Payment Channel Networks." 2022. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2022/115

[158] W. Yu, M. Xu, D. Yu, X. Cheng, Q. Hu, and Z. Xiong, "zk-PCN: A Privacy-Preserving Payment Channel Network Using zk-SNARKs," presented at the 2022 IEEE International Performance, Computing, and Communications Conference (IPCCC), IEEE Computer Society, Nov. 2022, pp. 57–64. doi: 10.1109/IPCCC55026.2022.9894329.

[159] L. Aumayr, K. Abbaszadeh, and M. Maffei, "Thora: Atomic and Privacy-Preserving Multi-Channel Updates." 2022. Accessed: Jul. 03, 2023. [Online]. Available: https://eprint.iacr.org/2022/317

[160] O. Osuntokun and C. Fromknecht, *Atomic multi-path payment*. 2018.

[161] G. van Dam and R. Abdul Kadir, "Hiding payments in lightning network with approximate differentially private payment channels," *Comput. Secur.*, vol. 115, p. 102623, Apr. 2022, doi: 10.1016/j.cose.2022.102623.

[162] L. Aumayr, P. Moreno-Sanchez, A. Kate, and M. Maffei, "Blitz: Secure {Multi-Hop} Payments Without {Two-Phase} Commits," presented at the 30th USENIX Security Symposium (USENIX Security 21), 2021, pp. 4043–4060. Accessed: Jul. 03, 2023. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/aumayr

[163] S. M. Abd Ali, M. N. Yusoff, and H. F. Hasan, "Redactable Blockchain: Comprehensive Review, Mechanisms, Challenges, Open Issues and Future Research Directions," *Future Internet*, vol. 15, no. 1, Art. no. 1, Jan. 2023, doi: 10.3390/fi15010035.