2024 Conference on Building a Secure & Empowered Cyberspace (BuildSEC)

2024 Conference on Building a Secure & Empowered Cyberspace (BuildSEC) | 979-8-3315-1672-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/BuildSEC64048.2024.00013

SoK: Payment Channel Networks

Kartick Kolachala, Mohammed Ababneh, Roopa Vishwanathan
New Mexico State University, USA
{kart1712, mababneh, roopav}@nmsu.edu

***Abstract*—Payment Channel Networks (PCNs) have been proposed as an alternative solution to the scalability, throughput, and cost overhead problems associated with blockchain transactions. By facilitating offchain execution of transactions, PCNs significantly reduce the burden on the blockchain, leading to faster transaction processing, reduced transaction fees, and enhanced privacy. Despite these advantages, the current state-of-the-art in PCNs presents a variety of challenges that require further exploration. In this paper, we survey several fundamental aspects of PCNs, such as pathfinding and routing, virtual channels, and payment channel hubs. We aim to provide the reader with a detailed understanding of the various aspects of PCN research, highlighting important advancements. Additionally, we highlight the various unresolved challenges in this area. Specifically, this paper seeks to answer the following crucial question: *What are the various interesting and non-trivial challenges in fundamental infrastructure design leading to efficient transaction processing in PCN research that require immediate attention from the academic and research community?* By addressing this question, we aim to identify the most pressing problems and future research directions, and we hope to inspire researchers and practitioners to tackle these challenges to make PCNs more secure and versatile.**

***Index Terms*—Payment channel networks, Layer-2, Routing, Virtual channels, Tumblers**

I. Introduction

Cryptocurrencies and cryptocurrency based transactions have become increasingly popular. Currently, the total market value of all cryptocurrencies in use has surpassed 2.5 Trillion USD, and the cryptocurrency market is increasing at a rate of $\approx$ 8.00% every year [1]. This rise in popularity can be attributed to the following reasons: 1) cryptocurrency transactions can be carried out without the presence of a trusted entity, while fiat currency based transactions require the presence of a trusted financial organization such as a bank. 2) cryptocurrency transactions do not subject the user to any limits on the number and type of transactions. Fiat currency based transactions are limited in their amount and number, depending on several factors such as the currency, geographical location, etc. [2].

Each transaction posted to the Bitcoin blockchain takes around 7 seconds to be validated [3]. The procedure of validation involves verifying that the transaction posted to the blockchain contains all the required fields and the signature of the user creating the transaction tuple is valid. Once the validation procedure is successfully completed, the transaction is included in a block that would be mined on the blockchain at some time in the future. The process of mining the block successfully takes $\approx$ 2 hours [3] (as of June 13^{th} 2024). This delay in the transactions and blocks getting confirmed is termed as the blockchain scalability problem. In contrast, Visa, a company which globally processes transactions using fiat currencies, processes around 24,000 transactions per second [4]. Due to the delay in transaction processing caused by the blockchain scalability problem, blockchain-based transactions cannot process payments instantaneously.

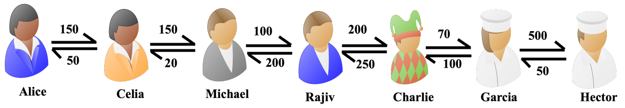


Figure 1: Payment channel network

As an alternative to processing transactions by posting to the blockchain, payment channels have been proposed. Two nodes with the intent of processing payments between them open a payment channel by creating a transaction tuple called the funding transaction. This funding transaction contains the initial deposits from both nodes. These initial deposits are also called as the initial balances of the nodes in the payment channel. The sum aggregate of these initial balances is called the channel capacity. The funding transaction contains the signatures of both the nodes involved in the payment channel making it a 2-2 multi signature transaction. This means that the funds in the funding transaction cannot be spent without the signatures of both nodes. This funding transaction is validated and included in a block. Once this block has been successfully mined and confirmed on the blockchain, the payment channel is opened between the two nodes. The two nodes can now be involved in an unlimited number of transactions with each other as long as the amount of a single transaction does not exceed their local balances.

The idea of a payment channel that exists between two nodes can be extended to a number of nodes, creating a network of payment channels, called a payment channel network or PCN. A PCN enables users (interchangeably called as nodes in the paper) that are not connected by a direct payment channel to make payments between each other in an off-chain manner. An example PCN is shown in Figure 1. In the figure, consider Alice who intends to make a payment to Hector, with whom she does not share a payment channel. The naïve way to process this transaction would for Alice to open a payment channel with Hector, which involves Alice making an expensive blockchain write for the channel opening. Each payment channel opening costs 2.4 USD for blockchain writes [5]. If Alice intends to send an amount of 1 coin to Hector,

979-8-3315-1672-7/24/$31.00 ©2024 IEEE
DOI 10.1109/BuildSEC64048.2024.00013

it may not be economical for her to open a direct payment channel. Alice can make use of the PCN and make a payment to Hector by forwarding the payment along the path Alice → Celia → Michael → Rajiv → Charlie → Garcia → Hector. This process of using intermediate nodes in a PCN to forward to the payment to the intended destination is called as routing in PCNs.

Motivation and timeliness of PCN research: A significant advantage of PCNs is their capability to facilitate micropayment transactions, with minimum amounts as low as 10^{-7} BTC [6]. In contrast, the average transaction cost for a single on-chain transaction on the BTC blockchain is approximately 4.612 USD as of June 2024 [7] regardless of the transaction amount. This cost can be avoided by using the off-chain PCNs, which incurs no additional fees. An example of a real-world PCN is the Lightning Network (LN) on the Bitcoin blockchain [8], which has a 24-hour trading volume of $63,200 and a market capitalization of $7 million [9] as of June 2024, indicating LN's growth.

Prior work: Prior works by Khojasteh *et al.* [10] and Erdin *et al.* [11] survey the work done only in the area of pathfinding and routing protocols and their privacy aspects in PCNs. Whereas, in this paper we cover a broader spectrum of PCN research: virtual channels and state channels, pathfinding and routing. Apart from this [10], [11] do not provide any information about the open problems in PCNs, which we do in our work. The SoK by Gudgeon *et al.* [12], surveys several layer-2 protocols, whereas, we focus exclusively on PCNs. Furthermore [12] was published in 2020 and does not cover most of the recent work published in PCNs.

In this SoK, we do not survey the various types of attacks in PCNs [13]–[19], [19]–[39]. The attacks in PCNs usually have overlaps in their strategy and execution, and most of them currently do not have efficient and fully developed mitigation mechanisms proposed. Our conjecture is that, their countermeasures might also have design overlaps as and when they are proposed. Hence, we believe attacks in PCNs and their countermeasures require their own taxonomy.

We have covered papers in various areas of PCNs during the time period of 2019-2024 across Tier-1, Tier-2, Tier-3 security conferences in CS, since the norm for security/privacy research and computer science research in general is peer-reviewed conferences.

Contributions:

1) We qualitatively compare the recent work in several aspects of building PCNs, viz. pathfinding and routing, virtual channels, and payment channel hubs using several relevant properties (metrics).

2) We point out the open problems in all the areas that we survey and we also discuss why solving those problems is a hard research challenge.

Outline: In Section II, we start with describing the concept of pathfinding and routing in PCNs and qualitatively compare work published in that area. In Section III, we describe virtual channels which have been proposed to address issues with multi-hop routing in PCNs, and compare work in this area. In Section IV, we cover payment channel hubs, which are similar to virtual channels but facilitate single hop payments to the receiver. In Section V, we present the reader with the current research gaps in all of the aforementioned areas and also describe why bridging those gaps is hard and in Section VI, we conclude the paper.

II. Pathfinding and Routing

Motivation: One of the areas in PCNs that has garnered significant attention from the academic community is pathfinding and routing. Pathfinding is defined as the process of finding a path comprising several nodes from a sender to a receiver in a PCN along which a payment can potentially be forwarded, and routing is the process of actually forwarding the payment along the found path. Intuitively, it may seem that well-known pathfinding and routing protocols from the wired and wireless networks domain can be easily applied to PCNs. Unfortunately, there are several problems with this: 1) Traditional networks focus on the transfer of data, PCNs on the other hand, transfer money in a decentralized manner. 2) Data transfer in traditional peer-peer networks does not alter the bandwidth, whereas money transfer in PCNs alters the monetary state of the nodes involved. 3) Cost in traditional networks is measured in terms of latency, whereas in PCNs, it involves routing fees, leading to greedy behavior among users and makes PCNs vulnerable to various attacks [12].

The properties on the columns in Table I represent the fundamental principles of fiat currency transactions and on-chain payment mechanisms, which we want reflected in off-chain payments. These properties are generally agreed upon in the literature by several works such as [40], [41], [43], [57]–[59] as common evaluation metrics for pathfinding and routing protocols in PCNs. Fulfilling these properties while providing efficient pathfinding and routing is a non-trivial challenge, and necessitates the design of new pathfinding and routing protocols. Several elegant pathfinding and routing protocols have been proposed in the literature. In Table I, we present a qualitative comparison of these routing protocols with respect to the properties they achieve. In this paper across all sections, if any prior work has identified a property as ideal or has identified a gap in research, we give an appropriate citation(s). If there is no citation provided, it indicates that the corresponding property/research gap has been identified by us.

Ideal properties: 1) **Concurrency**: Concurrency is achieved when a pathfinding and a routing protocol enables the nodes to forward more than one payment simultaneously [60]. 2) **Privacy**: Privacy is maintained when a node's real identity is known only to its immediate neighbors and not to the entire network. 3) **Topology privacy**: Topology privacy is preserved when no single node has knowledge of the entire network topology. 4) **Avoids source routing**: Source routing is avoided when the sender does not determine the path to the receiver. 5) **Decentralization**: Decentralization is achieved when there are no centralized, trusted entities responsible for constructing paths for senders. 6) **Atomicity**: Atomicity is ensured when the payment is routed all the way from the

Table I: Comparison of Pathfinding and Routing Protocols in PCNs

Protocols	Concurrency	Privacy	Topology privacy	Avoids source routing	Decentralized	Atomicity	Disjoint graphs	Fees	Year
SilentWhispers [40]	✗	✓	✓	✓	✓	✗	✗	✗	2017
SpeedyMurmurs [41]	✓	✓	✓	✓	✓	✗	✗	✗	2018
Coinexpress [42]	✓	✗	✓	✓	✓	✓	✗	✗	2018
Blanc [43]	✓	✓	✓	✓	✓	✓	✗	✗	2019
Robustpay [44]	✗	✗	✗	✗	✗	✓	✗	✓ (flat)	2019
Flash [45]	✗	✗	✗	✗	✗	✓	✗	✗	2019
Cheapay [46]	✗	✓	✓	✓	✓	✗	✗	✓ (flat)	2019
Eckey *et al* [47]	✗	✗	✓	✓	✓	✓	✗	✗	2020
FSTR [48]	✗	✗	✗	✗	✗	✗	✗	✗	2020
Spider [49]	✗	✗	✗	✗	✗	✗	✗	✗	2020
Vein [50]	✗	✗	✗	✗	✗	✗	✗	✓ (dynamic)	2021
Kadry *et al.* [51]	✗	✗	✗	✗	✗	✗	✗	✗	2021
Webflow [52]	✗	✓	✓	✓	✓	✗	✗	✗	2021
Robustpay+ [53]	✗	✗	✗	✗	✗	✓	✗	✓ (flat)	2021
MPCN-RP [54]	✗	✗	✗	✗	✗	✓	✗	✓ (flat)	2022
Auto tune [55]	✗	✗	✗	✗	✗	✗	✗	✓ (flat)	2023
Yang *et al.* [56]	✓	✓	✓	✓	✗	✗	✗	✗	2023
RACED [57]	✓	✓	✓	✓	✓	✓	✓	✗	2024
Auroch [58]	✓	✓	✓	✓	✓	✓	✗	✓ (dynamic)	2024
SPRITE [59]	✓	✓	✓	✓	✓	✓	✗	✗	2024

sender to the receiver, or the payment is not routed at all. 7) **Disjoint graphs**: A pathfinding and routing protocol is considered applicable to disjoint graphs if it functions even when the network graph consists of islands. A routing protocol should be able to facilitate transactions between any pair of nodes irrespective of their location. 8) **Fees**: Routing fees is the amount a node charges for forwarding the payment to the next node along a path from the sender to receiver. This fees can be charged in two ways. Flat/fixed fees means that the fees charged for routing payments remains the same irrespective of the transaction amount being routed. If the fees charged by a node varies according to the transaction amount, it is referred to as dynamic fees, typically a percentage of the amount.

As illustrated in Table I, routing protocols for payment channel networks (PCNs) have evolved significantly over the years. The two most significant advancements are taking routing fees into consideration and providing support for privacy. For instance, LN provides users with two sets of keys, a long-term keypair and an alias (a temporary identity) helping to conceal their identities and ensure privacy. Despite these developments, two overarching research problems remain that require attention. We discuss them in detail in Section V.

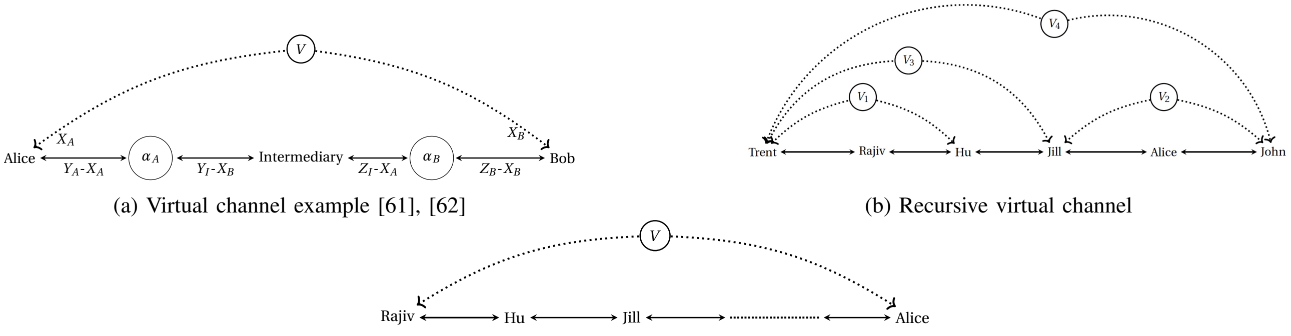
III. Virtual channels

Motivation: Transactions in PCNs are routed from the sender to the receiver using a path of intermediate nodes. Current pathfinding and routing mechanisms require the nodes along the payment path to be available for a transaction to be processed. However, nodes can sometimes choose to go offline or there can be network/service disconnections causing transaction failures. Furthermore, each node along a payment path charges its own fees for forwarding the payment, which is paid by the sender and increases with the path length, hence the time taken to route a payment grows linearly in the path length. Virtual channels, which are built on top of existing payment channels, solve these problems. Initial constructions of virtual channels facilitated payments between a pair of nodes using a single intermediate node [61]. The intermediate node needs to have individual payment channels open with the other two nodes. The intermediary and the pair of nodes lock coins with each other in their respective payment channels and a virtual channel is established. Upon establishment of virtual channel, the pair of nodes can be involved in a unlimited number of payments. These payments can be processed without the intermediate node being online. It might be better to use virtual channels from a routing fees perspective, since unlike routing protocols, nodes in virtual channels do not charge a routing fee for every transaction.

Alice, Bob, and an intermediary establish a virtual channel as shown in Figure 2a. Alice locks Y_A coins and the intermediary locks Y_I coins in the payment channel α_A. Similarly, Bob locks Z_B coins and the intermediary locks Z_I coins in their channel α_B. The virtual channel V is created once Alice locks X_A coins from her balance in α_A and Bob locks X_B coins from his balance in α_B. Now Alice and Bob can process payments without the intermediaries' online presence.

The idea of a virtual channel between a pair of nodes involving a single intermediary has been extended to establishing a virtual channel recursively over several hops involving several intermediaries, leading to the construction of a recursive virtual channel [65], [67], [68]. An example of a recursive channel is shown in the Figure 2b. A recursive virtual channel enables transaction processing between any pair of nodes, by recursively establishing virtual channels between several intermediaries, as opposed to Perun [61], which facilitates virtual channels only between a pair of nodes connected directly to an intermediary.

A multihop virtual channel is constructed by establishing a single virtual channel between a pair of users over a



(a) Virtual channel example [61], [62]

(b) Recursive virtual channel

(c) Multi-hop virtual channel (the dots between Jill and Alice depict several intermediate nodes)

Figure 2: Different types of virtual channels

Table II: Comparison of Virtual Channel Protocols

Protocol	BC	Validity	Fee	Privacy	Off-chain dispute resolution	Recursive	Multihop	Year
Generalized state channels [63]	TC	Limited	✗	✗	✗	✓	✗	2018
Eckey *et al.* [64]	TC	Limited	✗	✗	✗	✓	✗	2019
Perun [61]	TC	Limited	✗	✓	✗	✗	✗	2019
Jourenko *et al.* [65]	UTXO	Limited	✗	✗	✗	✗	✗	2020
Aumayr *et al.* [66]	UTXO	Limited	✓ (fixed)	✗	✗	✗	✗	2021
Elmo [67]	UTXO	Unlimited	✗	✗	✗	✓	✗	2021
Donner [68]	UTXO	Unlimited	✓ (time based)	✓	✗	✓	✗	2023
Jia *et al.* [69]	UTXO, TC	Limited	✓ (fixed)	✗	✗	✗	✗	2023

path comprising of several intermediate nodes. An example of multihop virtual channel is shown in the Figure 2c. A multihop virtual channel is an improvement over recursive virtual channels. In a multihop virtual channel, a single virtual channel can be established between any pair of nodes which are separated by several intermediaries.

Virtual channels should not add an unnecessary burden to users, and should mirror the operations of payment channels as closely as possible, with the added benefit of no on-chain transactions at all, while maintaining comparable security/privacy properties. We now give the properties desired from an ideal virtual channel, and compare the works in this area on the extent to which they achieve these properties.

Blockchain terminology: In the rest of the paper BC denotes a blockchain. TC is a blockchain that supports a Turing complete programming language, such as Ethereum, and UTXO is a blockchain that supports the UTXO-based scripting mechanism such as Bitcoin. In Table II, we present a qualitative comparison of virtual channel protocols.

Ideal properties: 1) **Validity**: This determines the validity of the virtual channel. A limited validity means that the virtual channel is valid for a predetermined time period (which is decided by nodes involved in the virtual channel). Unlimited validity means that the virtual channel can stay open until the nodes involved decide to initiate closing [64]. 2) **Fee**: This metric determines if the virtual channel takes into account the fees charged by the intermediate node(s) involved in the channel's establishment. The fixed fee model implies that a predetermined, fixed fee is paid to the intermediate node(s) which is agreed upon by all the nodes in the virtual channel before the channel establishment. The time-based fee model implies that the fee paid to the intermediary depends on the time for which the virtual channel stays open [64]. 3) **Privacy**: In any virtual channel construction, the real identity of a node should only be known to its immediate neighbor(s) [61]. 4) **Offchain dispute resolution**: This metric determines if the transaction disputes in a virtual channel require a blockchain write. 5) **Support for multihop virtual channels with several intermediaries**: A virtual channel is said to be multihop if it can facilitate payments between a sender and a receiver across a path comprising of several intermediate nodes by constructing a single virtual channel from the sender to the receiver, without establishing virtual channel between any pair of intermediate nodes along the path.

The most significant developments in virtual channels over the years are that newer protocols have incorporated a fees to be paid for the intermediary(ies) that lock coins in virtual channels and virtual channels now offer support for both TC based and UTXO based blockchains. Despite these developments, efficient virtual channel protocol design has three overarching research problems, which are discussed in Section V.

IV. Tumblers

Motivation: A payment channel hub (tumbler) is a multi-party off-chain system where users can establish payment channels with a central hub, which acts as an intermediary. It allows multiple users to send payments to each other without the need for direct payment channels between each user pair. The hub coordinates payments between different participants. The intermediary which facilitates payments is called a tumbler. Though a payment channel hub uses the same underlying infrastructure as that of PCNs and virtual channels, each of these constructions have their own use cases. PCNs are usually used when two nodes Alice and Bob transact on an infrequent basis. Virtual channels are used if Alice and Bob transact frequently, e.g., if Bob provides Alice with a service every month. Payment channel hubs are used when Alice needs to pay several receivers on a frequent basis and she does not want the tumbler to know the receivers.

Payment channel hubs can be classified into two types: on-chain and off-chain. On-chain payment channel hubs suffer from scalability issues due to having to post each transaction on the blockchain. Due to space constraints we describe on-chain hubs in the full version of the paper [80]. The scalability issues of on-chain payment channel hubs have led to the development of offchain payment channel hubs for specific blockchains, e.g., Bolt [70] for Zcash, Nocust [72] and MixCT [77] for Ethereum. The most general-purpose payment channel hubs are Tumblebit [71], A^2L [74], and Blindhub [79]. A payment channel hub should be able to facilitate payments between a sender and receiver, who do not have a payment channel open between them such that the hub cannot link a given transaction amount to a particular sender/receiver pair. Furthermore, the payment channel hub should also guarantee the fundamental property of atomicity (ensuring that the payment is sent to the receiver or it does not go through at all). We now give the properties desired from an ideal payment channel hub, and compare the works in this area on the extent to which they achieve these properties. In Table III, we qualitatively compare several off-chain tumblers.

Ideal properties: 1) **Relationship anonymity**: It ensures that the relationship between a sender and a receiver for a given transaction should not be known to the tumbler [70]. 2) **Privacy against aborts**: Tumbler should not be able to deduce the identities of a sender/receiver in case of a transaction abort, regardless of which party is responsible for the abort [79]. Aborts can happen due to several reasons such as network disconnections, power outages, etc. Malicious nodes can also deliberately abort a protocol. In the case of tumbler protocols, the nodes whose payments did not succeed can be linked to each other once the protocol execution completes. 3) **Independent of time epochs**: The tumbler processes transactions in discrete fragments of time called epochs, i.e., transactions only take place during a time epoch [70]. This is not ideal. 4) **Protection against dynamic corruption of nodes**: Current tumbler protocols corrupt nodes at the beginning of protocol execution and assume that the set of corrupted nodes remains constant until the protocol execution terminates. Ideally, a payment channel hub should be able to handle the deviation of any party from the protocol at any point during its execution. 5) **Atomicity**: Atomicity is ensured if either the payment is routed all the way from the sender to the receiver or the payment is routed at all. 6) **Value privacy**: Value privacy is ensured by a payment channel hub, when, given a transaction amount, the tumbler cannot link it to a sender/receiver pair [70]. 7) **Variable amount**: The tumbler should be able to process transactions of any amount [70].

Over the years, various payment channel hub constructions have been developed to address specific challenges based on their unique design goals. However, we have identified three overarching research problems in payment channel hubs that require attention. We discuss them in Section V.

There are two other designs which are of fundamental importance in PCNs: state channels and rebalancing protocols. Due to space constraints, we discuss them in the full version of the paper [80].

V. Research Gaps & Open Problems

In this section, we highlight the gaps in research published up until now in the areas of pathfinding and routing, virtual channel construction, and payment channel hubs. The gaps are described as research questions, denoted by **RQ**.

RQ1: Why is super node liquidity validation in PCNs hard? A super node, variously called as a trampoline node, routing node, routing helper, landmark node, router, etc. [40], [43], [49], [57], [59] is a highly connected node with numerous high liquidity channels, that helps in pathfinding and routing payments. One of the main problems with the super nodes is that a sender has of knowing whether the super node possesses enough liquidity on its channels to route a payment. The local balance of a super node in a given channel (or of any node in a PCN) is a private value and should not be known to any node except for its immediate neighbor(s). Currently, if a super node does not have enough liquidity to route a transaction, the transaction fails and it has to be retried by the sender. In LN, one of the most widely used PCN, this is a significant problem. Sometimes the sender might have to keep retrying for ≈ 1 hour to have a successful payment [81]. The main goal of PCNs is to facilitate instantaneous payments and these transaction retries render such payments almost impossible. It will greatly benefit the sender if there is a mechanism to validate whether a super node has enough liquidity (balance) to route its payment without violating any privacy concerns.

RQ2: Why is channel verification in a PCN hard? To be a part of any PCN, nodes will open payment channels with other nodes in the network. Two nodes open a payment channel between them by posting a transaction to the blockchain. This transaction can be posted on the blockchain or as a function

Table III: Comparison of Payment Channel Hubs

Protocol	BC	Relationship anonymity	Privacy against aborts	Independent of epochs	Dynamic corruption	Atomicity	Value privacy	Variable amount	Year
BOLT [70]	TC	✓	✗	✓	✗	✓	✓	✓	2017
Tumblebit [71]	UTXO	✓	✗	✗	✗	✓	✗	✗	2017
Nocust [72]	TC	✓	✗	✗	✗	✓	✗	✓	2018
Teechain [73]	TC	✓	✗	✗	✗	✓	✓	✓	2019
A^2L [74]	UTXO, TC	✓	✗	✗	✗	✓	✓	✗	2021
Accio [75]	TC	✓	✓	✓	✗	✓	✓	✓	2021
Boros [76]	TC	✗	✗	✓	✗	✓	✗	✓	2021
MIXCT [77]	TC	✓	✗	✗	✗	✓	✓	✓	2022
Turbo [78]	TC	✓	✗	✗	✗	✗	✗	✗	2022
Blindhub [79]	UTXO, TC	✓	✗	✗	✗	✓	✓	✓	2023

call to an existing smart contract. In the most popular PCN, LN, the procedure of verifying whether a payment channel really exists on the blockchain is very inefficient. A node who wants to verify a channel needs to request the block in which the channel opening transaction has been included, verifying whether the transaction has been successfully executed by the validator/miner and finally verifying if the channel opening transaction corresponds to a 2-2 multi signature address on the blockchain. The verifier performing these steps is inefficient since all these steps will have already been performed by the miner. Finding a way to do this without blockchain access and in a blockchain agnostic manner in a hard research challenge.

RQ3: Why is designing pathfinding protocols for PCNs, that comprise of several distinct well-connected components a hard problem? Though solutions such as [57] exist that solve this problem to a certain extent by using routing helpers/trampoline nodes, the aspect that makes it hard is to quantify the denseness/sparseness of a well-connected component. If we assume that we deploy one trampoline node for each well-connected component, there may be well-connected components in the PCN which only have a few nodes (i.e., islands). Selection of a trampoline node amongst these nodes is difficult.

RQ4: Why is designing a routing protocol that supports concurrent payments and is resilient to channel gaming a hard problem? Processing concurrent transactions requires the design of a mechanism that allows a node to lock a portion of its liquidity in a channel with an immediate neighbor for one transaction while simultaneously using the remaining liquidity to process another. Though there are protocols that support concurrency [40], [42], [43], [57]–[59], they are not resilient to the presence of potentially malicious nodes in the PCN, which may initiate transactions with the sole intent of locking liquidity, leading to congestion and disruption in the network.

RQ5: Why is having a well-defined fee structure for virtual channels hard? The intermediary(s) involved in the virtual channel construction additionally lock coins in virtual channels apart from the ones locked in the underlying payment channel. Currently, nodes get paid routing fees for every transaction they process. In the case of virtual channels, having a well-defined fee structure is difficult due to the following reasons: 1) The fee structure should take into account the amount of funds and the time for which these funds of the intermediary(ies) are locked in a virtual channel. 2) It also needs to take into account the routing fee an intermediary could have earned by not locking up the coins in the virtual channel.

RQ6: Why is off-chain dispute resolution in virtual channels hard? There is no offchain consensus mechanism for dispute resolution in a PCN, as opposed to the 51% honest majority assumption that exists among validators on the blockchain. This honest majority helps resolve disputes in the transactions posted to the blockchain. Designing such a dispute mechanism for layer-2 transactions is hard since transactions are private (not posted to the blockchain), and nodes do not broadcast their activities to the entire network.

RQ7: Why is providing support for a multihop virtual channel a hard problem? This is hard since a multi-hop virtual channel construction should ensure that neither sender/receiver nor the intermediate nodes should lock coins in multiple channels at the same time.

RQ8: Why is ensuring privacy in a virtual channel protocol a hard problem? In a recursive virtual channel, new virtual channels are constructed on top of existing virtual channels to facilitate payments. This staggered nature makes it mandatory to reveal the identity of at least one endpoint node (sender or receiver). This is because, at least one node among the sender/receiver is involved in all virtual channels. The solution to this problem is to design a multihop virtual channel.

RQ9: Why is designing a payment channel hub (PCH) that is resistant to privacy against aborts and dynamic corruption a hard challenge? PCHs usually use transaction mixing for enhancing privacy, which is a process in which multiple payments from different users are mixed together in such a way that it is infeasible for the hub to link the sender and recipient of a specific transaction. This process helps obscure the flow of funds, providing unlinkability. Designing a payment channel hub that is resistant to privacy against aborts is hard because, if a PCH selectively aborts a payment from a sender/receiver, the counter party whose payment also failed can be linked. If sender/receiver gets corrupted during the PCH's execution, the corresponding transaction has to be aborted to ensure atomicity, which is why the existing tumbler constructions assume a static adversary, in which certain nodes are designated as corrupted before the PCH begins execution. The trade off here is preserving transaction unlikability during a corrupted party's transaction abort.

VI. Conclusion

In this paper, we qualitatively compared the recent work in various foundational areas of PCN research: pathfinding and routing, virtual channels, and payment channel hubs. We also discussed the gaps in research in these areas along with reasons why fulfilling those gaps is non-trivial. We hope that this paper motivates researchers to build robust protocols that address these gaps that would go a long way towards building out and developing a decentralized financial ecosystem.

Acknowledgement

This material is based upon work supported by the National Science Foundation under Award No. 2148358, 1914635, 2417062, and the Department of Energy under Award No. DE-SC0023392. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation and the Department of Energy.

References

[1] "Top cryptocurrency statistics and trends in 2024," https://bit.ly/3WnCkYE.

[2] Nerdwallet, "Xoom money transfer review," https://bit.ly/3QnPOAu.

[3] "Btc confirmation time," https://bit.ly/3AhRlnf.

[4] "Visa," https://bit.ly/4dszZ5v.

[5] Medium, "How to calculate bitcoin transaction fees: What businesses need to know about bitcoin," https://bit.ly/3ygDZqN.

[6] MIT, "layer 2 the lightning network," https://dci.mit.edu/lightning-network.

[7] BTC, "Bitcoin average transaction fee," https://bit.ly/4djgHQ6.

[8] LND, "Lnd," https://docs.lightning.engineering, 2023.

[9] coinmarket, "Ln trading volume," https://bit.ly/3Yo6EEU.

[10] H. Khojasteh and H. Tabatabaei, "A survey and taxonomy of blockchain-based payment channel networks," in *2021 IEEE High Performance Extreme Computing Conference (HPEC)*. IEEE, pp. 1–8.

[11] E. Erdin, S. Mercan, and K. Akkaya, "An evaluation of cryptocurrency payment channel networks and their privacy implications. arxiv 2021," *arXiv preprint arXiv:2102.02659*.

[12] L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais, "Sok: Layer-two blockchain protocols," in *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24*. Springer, pp. 201–226.

[13] Z. Avarikioti, P. Kdzior, T. Lizurej, and T. Michalak, "Bribe & fork: Cheap bribing attacks via forking threat," *arXiv preprint arXiv:2402.01363*, 2024.

[14] B. Weintraub, S. P. Kumble, C. Nita-Rotaru, and S. Roos, "Payout races and congested channels: A formal analysis of security in the lightning network," *arXiv preprint arXiv:2405.02147*, 2024.

[15] T. Von Arx, M. Tran, and L. Vanbever, "Revelio: A network-level privacy attack in the lightning network," in *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*. IEEE, pp. 942–957.

[16] A. A. Khalil, M. A. Rahman, and H. A. Kholidy, "Fakey: Fake hashed key attack on payment channel networks," in *2023 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2023, pp. 1–9.

[17] S. Mazumdar, P. Banerjee, A. Sinha, S. Ruj, and B. K. Roy, "Strategic analysis of griefing attack in lightning network," *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1790–1803, 2022.

[18] C. Sguanci and A. Sidiropoulos, "Mass exit attacks on the lightning network," in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023, pp. 1–3.

[19] C. Shikhelman and S. Tikhomirov, "Unjamming lightning: A systematic approach," *Cryptology ePrint Archive*, 2022.

[20] A. Biryukov, G. Naumenko, and S. Tikhomirov, "Analysis and probing of parallel channels in the lightning network," in *International Conference on Financial Cryptography and Data Security*. Springer, 2022, pp. 337–357.

[21] A. Riard and G. Naumenko, "Time-Dilation Attacks on the Lightning Network," *Cryptoeconomic Systems*, vol. 1, no. 2, oct 22 2021.

[22] A. Mizrahi and A. Zohar, "Congestion attacks in payment channel networks," in *International conference on financial cryptography and data security*. Springer, 2021, pp. 170–188.

[23] B. Weintraub, C. Nita-Rotaru, and S. Roos, "Structural attacks on local routing in payment channel networks," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, pp. 367–379.

[24] C. Pérez-Sola, A. Ranchal-Pedrosa, J. Herrera-Joancomartí, G. Navarro-Arribas, and J. Garcia-Alfaro, "Lockdown: Balance availability attack against lightning network channels," in *Financial Cryptography and Data Security: 24th International Conference*. Springer, 2020, pp. 245–263.

[25] 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*, 2020, pp. 202–213.

[26] S. Tochner, A. Zohar, and S. Schmid, "Route hijacking and dos in off-chain networks," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 2020, pp. 228–240.

[27] S. Mazumdar, P. Banerjee, and S. Ruj, "Griefing-penalty: Countermeasure for griefing attack in lightning network," *arXiv preprint arXiv:2005.09327*, 2020.

[28] E. Rohrer and F. Tschorsch, "Counting down thunder: Timing attacks on privacy in payment channel networks," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 2020, pp. 214–227.

[29] Z. Lu, R. Han, and J. Yu, "General Congestion Attack on HTLC-Based Payment Channel Networks," in *3rd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2021)*, ser. Open Access Series in Informatics (OASIcs), V. Gramoli, H. Halaburda, and R. Pass, Eds., vol. 97. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022, pp. 2:1–2:15.

[30] G. Van Dam, R. A. Kadir, P. N. Nohuddin, and H. B. Zaman, "Improvements of the balance discovery attack on lightning network payment channels," in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2020, pp. 313–323.

[31] E. Rohrer, J. Malliaris, and F. Tschorsch, "Discharged payment channels: Quantifying the lightning network's resilience to topology-based attacks," in *2019 IEEE european symposium on security and privacy workshops (EuroS&PW)*. IEEE, pp. 347–356.

[32] M. Romiti, F. Victor, P. Moreno-Sanchez, P. S. Nordholt, B. Haslhofer, and M. Maffei, "Cross-layer deanonymization methods in the lightning protocol," in *International Conference on Financial Cryptography and Data Security*. Springer, 2021, pp. 187–204.

[33] 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)*, pp. 387–396.

[34] T. von Arx, M. Tran, and L. Vanbever, "Revelio: A network-level privacy attack in the lightning network," in *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, pp. 942–957.

[35] G. Kappos, H. Yousaf, A. Piotrowska, S. Kanjalkar, S. Delgado-Segura, A. Miller, and S. Meiklejohn, "An empirical analysis of privacy in the lightning network," in *Financial Cryptography and Data Security: 25th International Conference, FC 2021*. Springer, pp. 167–186.

[36] P. Kumar Sharma, D. Gosain, and C. Diaz, "On the anonymity of peer-to-peer network anonymity schemes used by cryptocurrencies," in *The Network and Distributed System Security Symposium*. Internet Society, 2023.

[37] P. Zabka, K.-T. Foerster, C. Decker, and S. Schmid, "Short paper: A centrality analysis of the lightning network," in *International Conference on Financial Cryptography and Data Security*. Springer, 2022, pp. 374–385.

[38] P. Casas, M. Romiti, P. Holzer, S. B. Mariem, B. Donnet, and B. Haslhofer, "Where is the light(ning) in the taproot dawn? unveiling the bitcoin lightning (ip) network," in *2021 IEEE 10th International Conference on Cloud Networking (CloudNet)*, 2021, pp. 87–90.

[39] L. Heimbach, Y. Vonlanthen, J. Villacis, L. Kiffer, and R. Wattenhofer, "Deanonymizing ethereum validators: The p2p network has a privacy issue," *arXiv preprint arXiv:2409.04366*, 2024.

[40] G. Malavolta, P. Moreno-Sanchez, A. Kate, and M. Maffei, "Silentwhispers: Enforcing security and privacy in decentralized credit networks," in *24th Annual Network and Distributed System Security Symposium, NDSS*, 2017.

[41] S. Roos, P. Moreno-Sanchez, A. Kate, and I. Goldberg, "Settling payments fast and private: Efficient decentralized routing for path-based transactions," in *25th Annual Network and Distributed System Security Symposium, NDSS*, 2018.

[42] 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 *27th International Conference on Computer Communication and Networks, ICCCN 2018*. IEEE, pp. 1–9.

[43] G. Panwar, S. Misra, and R. Vishwanathan, "Blanc: Blockchain-based anonymous and decentralized credit networks," in *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, ser. CODASPY '19. Association for Computing Machinery, p. 339–350.

[44] Y. Zhang and D. Yang, "Robustpay: Robust payment routing protocol in blockchain-based payment channel networks," in *2019 IEEE 27th International Conference on Network Protocols (ICNP)*, pp. 1–4.

[45] P. Wang, H. Xu, X. Jin, and T. Wang, "Flash: Efficient dynamic routing for offchain networks," ser. CoNEXT '19. Association for Computing Machinery, 2019, p. 370–381.

[46] 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)*, pp. 1–6.

[47] L. Eckey, S. Faust, K. Hostáková, and S. Roos, "Splitting payments locally while routing interdimensionally," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 555, 2020.

[48] 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)*, pp. 464–475.

[49] V. Sivaraman, S. B. Venkatakrishnan, K. Ruan, P. Negi, L. Yang, R. Mittal, G. Fanti, and M. Alizadeh, "High throughput cryptocurrency routing in payment channel networks," in *17th USENIX Symposium on Networked Systems Design and Implementation*, 2020, pp. 777–796.

[50] Q. Gong, C. Zhou, L. Qi, J. Li, J. Zhang, and J. Xu, "Vein: High scalability routing algorithm for blockchain-based payment channel networks," in *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2021, pp. 43–50.

[51] H. Kadry and Y. Gadallah, "A machine learning-based routing technique for off-chain transactions in payment channel networks," in *2021 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pp. 66–73.

[52] X. Zhang, S. Shi, and C. Qian, "Webflow: Scalable and decentralized routing for payment channel networks with high resource utilization," *CoRR*, vol. abs/2109.11665, 2021.

[53] Y. Zhang and D. Yang, "Robustpay+: Robust payment routing with approximation guarantee in blockchain-based payment channel networks," *IEEE/ACM Transactions on Networking*, vol. 29, pp. 1676–1686, 2021.

[54] Y. Chen, Y. Ran, J. Zhou, J. Zhang, and X. Gong, "Mpcn-rp: A routing protocol for blockchain-based multi-charge payment channel networks," *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, pp. 1229–1242, 2022.

[55] H.-J. Hong, S.-Y. Chang, and X. Zhou, "Auto-tune: An efficient autonomous multi-path payment routing algorithm for payment channel networks," *Computer Networks*, vol. 225, p. 109659, 2023.

[56] L. Yang, X. Dong, S. Gao, Q. Qu, X. Zhang, W. Tian, and Y. Shen, "Optimal hub placement and deadlock-free routing for payment channel network scalability," in *2023 IEEE 43rd International Conference on Distributed Computing Systems (ICDCS)*.

[57] K. Kolachala, M. Ababneh, and R. Vishwanathan, "Raced: Routing in payment channel networks using distributed hash tables," in *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, ser. ASIA CCS '24. Association for Computing Machinery, p. 1895–1910.

[58] M. Ababneh, K. Kolachala, and R. Vishwanathan, "Auroch: Auction-based multipath routing for payment channel networks," in *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, ser. ASIA CCS '24. Association for Computing Machinery, p. 1861–1877.

[59] G. Panwar, R. Vishwanathan, G. Torres, and S. Misra, "Sprite: Secure and private routing in payment channel networks," in *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*. Association for Computing Machinery, p. 1878–1894.

[60] 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*, pp. 455–471.

[61] S. Dziembowski, L. Eckey, S. Faust, and D. Malinowski, "Perun: Virtual payment hubs over cryptocurrencies," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, pp. 106–123.

[62] K. Kolachala, E. Simsek, M. Ababneh, and R. Vishwanathan, "Sok: Money laundering in cryptocurrencies," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ser. ARES '21. Association for Computing Machinery, 2021.

[63] S. Dziembowski, S. Faust, and K. Hostáková, "General state channel networks," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 949–966.

[64] S. Dziembowski, L. Eckey, S. Faust, J. Hesse, and K. Hostáková, "Multi-party virtual state channels," in *Advances in Cryptology–EUROCRYPT 2019*. Springer, pp. 625–656.

[65] M. Jourenko, M. Larangeira, and K. Tanaka, "Lightweight virtual payment channels," in *International Conference on Cryptology and Network Security*. Springer, 2020, pp. 365–384.

[66] L. Aumayr, M. Maffei, O. Ersoy, A. Erwig, S. Faust, S. Riahi, K. Hostáková, and P. Moreno-Sanchez, "Bitcoin-compatible virtual channels," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 901–918.

[67] A. Kiayias and O. S. T. Litos, "Elmo: Recursive virtual payment channels for bitcoin," *Cryptology ePrint Archive*, 2021.

[68] L. Aumayr, P. Moreno-Sanchez, A. Kate, and M. Maffei, "Breaking and fixing virtual channels: Domino attack and donner," in *Network and Distributed System Security (NDSS) Symposium*, 2023.

[69] 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.

[70] 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*, pp. 473–489.

[71] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "Tumblebit: An untrusted bitcoin-compatible anonymous payment hub," in *Network and distributed system security symposium*, 2017.

[72] R. Khalil, A. Zamyatin, G. Felley, P. Moreno-Sanchez, and A. Gervais, "Commit-chains: Secure, scalable off-chain payments," *Cryptology ePrint Archive*, 2018.

[73] 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*, 2019, pp. 63–79.

[74] 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)*, 2021, pp. 1834–1851.

[75] Z. Ge, J. Gu, C. Wang, Y. Long, X. Xu, and D. Gu, "Accio: Variable-amount, optimized-unlinkable and nizk-free off-chain payments via hubs," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '23. Association for Computing Machinery, p. 1541–1555.

[76] J. Zhang, Y. Ye, W. Wu, and X. Luo, "Boros: Secure and efficient off-blockchain transactions via payment channel hub," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 407–421, 2021.

[77] J. Du, Z. Ge, Y. Long, Z. Liu, S. Sun, X. Xu, and D. Gu, "Mixct: Mixing confidential transactions from homomorphic commitment," in *European Symposium on Research in Computer Security*. Springer, 2022, pp. 763–769.

[78] J. He, W. Qiu, R. He, S. Zhuo, and W. Jie, "Turbo: A high-performance and secure off-chain payment hub," in *International Conference on Machine Learning for Cyber Security*. Springer, 2022, pp. 67–75.

[79] X. Qin, S. Pan, A. Mirzaei, Z. Sui, O. Ersoy, A. Sakzad, M. F. Esgin, J. K. Liu, J. Yu, and T. H. Yuen, "Blindhub: Bitcoin-compatible privacy-preserving payment channel hubs supporting variable amounts," in *2023 IEEE Symposium on Security and Privacy (SP)*, pp. 2462–2480.

[80] K. Kolachala, M. Ababneh, and R. Vishwanathan, "Sok: Payment channel networks," *arXiv preprint arXiv:2407.20968*, 2024.

[81] ACINQ, "Trampoline fee insufficient," https://bit.ly/4fvJN0A.