SoK: Layer-Two Blockchain Protocols

Gudgeon, Lewis; Moreno-Sanchez, Pedro; Roos, Stefanie; McCorry, Patrick; Gervais, Arthur

DOI
10.1007/978-3-030-51280-4_12

Publication date
2020

Published in
Financial Cryptography and Data Security - 24th International Conference, FC 2020, Revised Selected Papers

Citation (APA)
Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2020). SoK: Layer-Two Blockchain Protocols. In J. Bonneau, & N. Heninger (Eds.), *Financial Cryptography and Data Security - 24th International Conference, FC 2020, Revised Selected Papers* (Vol. 12059, pp. 201-226). (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Vol. 12059 LNCS). https://doi.org/10.1007/978-3-030-51280-4_12

SoK: Layer-Two Blockchain Protocols

Lewis Gudgeon[1], Pedro Moreno-Sanchez[2], Stefanie Roos[3], Patrick McCorry[4], and Arthur Gervais[1,5,6]

[1] Imperial College London, United Kingdom
[2] TU Wien, Austria
[3] TU Delft, Netherlands
[4] PISA Research, United Kingdom
[5] Lucerne University of Applied Sciences and Arts, Switzerland
[6] Liquidity Network, Switzerland

Abstract. Blockchains have the potential to revolutionize markets and services. However, they currently exhibit high latencies and fail to handle transaction loads comparable to those managed by traditional financial systems. *Layer-two* protocols, built on top of (*layer-one*) blockchains, avoid disseminating every transaction to the whole network by exchanging authenticated transactions *off-chain*. Instead, they utilize the expensive and low-rate blockchain only as a recourse for disputes. The promise of layer-two protocols is to complete off-chain transactions in sub-seconds rather than minutes or hours while retaining asset security, reducing fees and allowing blockchains to scale.
We systematize the evolution of layer-two protocols over the period from the inception of cryptocurrencies in 2009 until today, structuring the multifaceted body of research on layer-two transactions. Categorizing the research into payment and state channels, commit-chains and protocols for refereed delegation, we provide a comparison of the protocols and their properties. We provide a systematization of the associated synchronization and routing protocols along with their privacy and security aspects. This Systematization of Knowledge (SoK) clears the layer-two fog, highlights the potential of layer-two solutions and identifies their unsolved challenges, indicating propitious avenues of future work.

Keywords: Applied Cryptography, Blockchain Applications, Layer-Two Blockchain Protocols, Blockchain Scaling, Cryptocurrency Adoption

1 Introduction

Blockchains offer a mechanism through which mutually mistrusting entities can cooperate in the absence of a trusted third party. However, the permissionless nature of their consensus algorithms (i.e. where no third party is entrusted with the safekeeping of funds) limits their scalability to about ten transactions-per-second (tps) [1, 2], far fewer than custodian payment systems offering thousands of tps [3]. These scaling issues have led to a rich literature corpus exploring different blockchain scaling solutions: (i) alternative blockchain consensus architectures [4–13], (ii) sharding [14–18] and (iii) side-chains [19], some of which

were systematized in related work [20]. However, modifying a consensus mechanism implies changing one of the key elements of a blockchain system while already in-use, which creates crucial issues such as a lack of backward compatibility, clearly hindering their implementation in practice. Additionally, consensus changes might even lead to different, forked systems [21].

Layer-two protocols are an orthogonal scaling solution. Contrary to the aforementioned solutions, layer-two protocols scale blockchains *without* changing the layer-one trust assumptions and they do not extend or replace the consensus mechanism. Layer-two protocols enable users to perform so-called *off-chain* transactions through private and authenticated communication, rather than broadcasting every single transaction on the (parent) blockchain. This optimization reduces the transaction load on the underlying blockchain and is fully backward compatible. The theoretical transaction throughput is only bounded by the communication bandwidth and latency of the involved parties. Off-chain transaction security can be guaranteed via allocated collateral, e.g. in payment channel designs [22–25] or by offering delayed transaction finality in commit-chain proposals [26].

A rich body of literature has emerged on off-chain protocols, proposing payment [22–25, 27], state [28] and virtual [29] channels, payment channel networks (PCNs) [25, 27] and related routing protocols [30–35], channel rebalancing [36] and channel factories [37] constructions, commit-chains [26, 38], channel hubs [39, 40], privacy-enhancing channels [39, 41–43] and protocols for refereed delegation [44,45]. However, the sources of information about layer-two protocols are highly disparate. Moreover, in part due to the rapid pace of advancement in the blockchain field, we observe, mostly outside academia, a frequent underspecification of constructions and their adversarial assumptions. This makes it exceedingly difficult to discern thought-through concepts from marketing activities. We aim to clear the fog surrounding layer-two protocols, equipping newcomers to this inaccessible field with a concise reference, and inform the directions of future work. This Systematization of Knowledge (SoK) provides a systematic overview of layer-two systems since the inception of cryptocurrencies in 2009 and identifies the complete set of proposed layer-two protocol types.

This SoK is structured as follows. Section 2 outlines the necessary background followed by different layer-two design classes, *channels* in Section 3, *commit-chains* in Section 4 and *protocols for refereed delegation* in Section 5. For completeness, Section 6 presents two sets of complementary approaches to layer-two protocols. Section 7 considers the anonymity and privacy aspects of layer-two protocols, Section 8 covers security properties and we conclude the paper in Section 9.

2 Blockchains and Off-Chain Transactions

This section establishes the necessary background and isolates the blockchain components relevant to layer-two. The background presented here is necessarily not a complete overview of blockchain-related concepts, which have been surveyed in other SoKs [20, 46]. We distinguish between four different layers within

a blockchain system: the *hardware*, *layer-zero*, *layer-one* and *layer-two* (cf. Figure 1).

Hardware Layer. Trusted Execution Environments (TEE) substitute the need for a blockchain clock with a trusted hardware assumption, thus enabling efficient protocols at other layers such as off-chain payments [47, 48], the removal of dispute processes and backward compatibility [49]. TEE (e.g. Intel SGX) execute sensitive or security-critical application code within *enclaves* [50, 51], tamper-proof from the operating system or other higher-privileged software.

The Network Layer. The network layer, or layer-zero, is typically a peer-to-peer layer on which blockchain nodes exchange information asynchronously [52]. The network layer is of utmost importance to the scalability [53, 54], security [1] and privacy [55] of a blockchain. An efficient layer-zero enables higher transaction throughput and stronger resilience against malicious actors [1]. Blockchain miners, who write transactions to the blockchain, are connected through dedicated *miner* P2P networks (e.g. Fibre [56]), in addition to the public blockchain P2P network. Note that the network layer encompasses the complete network stack of the traditional network architecture rather than only the classical network layer, which focuses Internet routing. More concretely, the network layer should provide reliable communication between two participants in a blockchain.

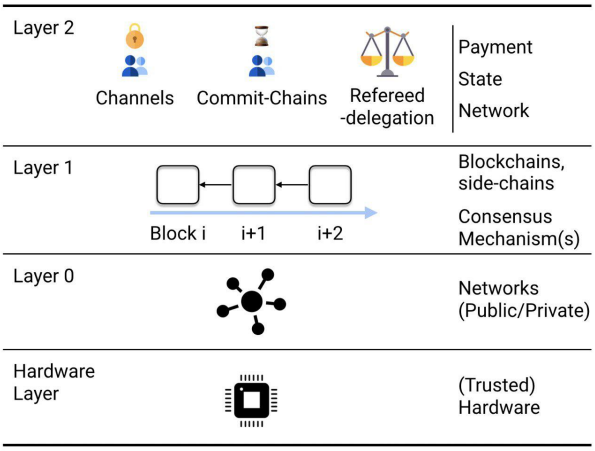

Fig. 1. Suggested blockchain layers. Layer-two channels and commit-chains operate without additional consensus mechanism and transact payments, state, and spawn networks.

The Blockchain Layer. Layer-one hosts an immutable append-only chain of blocks that accumulates transactions from parties in a network for public verifiability [46]. Each transaction encodes an update of the state of the blockchain. A transaction can exchange digital assets between parties or invoke an application (i.e. smart contract). The integrity of the blockchain is ensured by means of a consensus algorithm executed across participants. Consensus algorithms rely on e.g. the computationally expensive Proof-of-Work (PoW) [13, 57–60] or a large number of alternatives [8, 9, 61–65]. Blockchains can be permissionless or permissioned depending on whether participation is open or restricted. We focus on permissionless blockchains as permissioned blockchains lack the non-custodial

property, but layer-two concepts apply equally to permissioned blockchains. Crucial for the design of layer-two protocols is the scripting language of the underlying blockchain. Bitcoin-like blockchains are based on a restricted Script language [57] and operate via a set of Unspent Transaction Outputs (UTXO), while other blockchains support Turing-complete languages enabling highly expressive smart contracts [66]. Layer-two protocols typically assume two properties from the blockchain layer: *integrity* (i.e. only valid transactions are added to the ledger) and *eventual synchronicity with an upper time-bound* (i.e. a valid transaction is eventually added to the ledger, before a critical timeout).

We informally define off-chain or layer-two protocols as follows.

Definition 1. *(Layer-two protocols). A layer-two protocol allows transactions between users through the exchange of authenticated messages via a medium which is outside of, but tethered to, a layer-one blockchain. Authenticated assertions are submitted to the parent-chain only in cases of a dispute, with the parent-chain deciding the outcome of the dispute. Security and non-custodial properties of a layer-two protocol rely on the consensus algorithm of the* parent-chain.

Off-chain protocols can be categorized into in three principal flavors: (i) channels, which are formed between n coequal parties (Section 3, e.g., [25, 27]); (ii) commit-chains, which rely on one central intermediary, trusted regarding availability but untrusted regarding funds. (Section 4, e.g. [26,67]); and (iii) protocols for refereed delegation (Section 5, e.g. [44, 45]). While side-chains [19] let parties transact on a distinct blockchain, they do not classify as layer-two due to having their own consensus algorithm.

3 Channels

In this section we first provide an account of the evolution of channel constructions (sections 3.1 to 3.4), including the requirement for new watching services (section 3.3), before considering how multiple single channels can be synchronized (section 3.5); the routing challenges that synchronized channels present (section 3.6); and finally the construction of payment channel hubs (section 3.7).

3.1 Channel Overview

A channel establishes a private peer-to-peer medium, governed by pre-set rules, e.g. a smart contract, allowing the involved parties to consent to state updates unanimously by exchanging authenticated state transitions off-chain. We provide an overview of state-of-the-art channel constructions in Appendix G Table A1 where we distinguish between two channel techniques: (i) *payment channels*, supporting off-chain payment interactions; and (ii) *state channels*, supporting off-chain arbitrary interactions.

Payment channels emerged [22] to support rapid one-way payments, then transitioned towards bi-directional channel designs [25], where both parties can issue and receive payments. *State channels* [28] generalize the concept to support the execution of arbitrary state transitions. A state channel allows n parties to agree, via *unanimous* consent, to a new state of a previously agreed smart

contract. A channel's lifetime consists of three phases: *(i)* channel establishment, *(ii)* transition and *(iii)* channel closure or disputes[7].

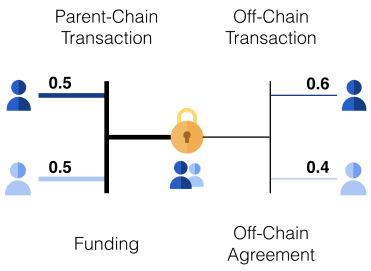

Fig. 2. Payment channel funding (UTXO model) and off-chain transaction.

Channel Establishment. All parties cooperatively *open* a channel by locking collateral on the blockchain (cf. Figure 2). The funds can only be released by unanimous agreement or through a pre-defined refund condition.

Channel Transitions. Once the channel is open, all parties can *update* the channel's state in a two-step process. First, one party proposes a new state transition by sending a signed command and the new $state_i$ to all other parties. Each party computes the state transition as $state_i \leftarrow T_\alpha(state_{i-1}, cmd_\alpha)$, where T_α denotes the transition function for application α and cmd_α denotes a given command relevant to application α. Second, all other parties re-compute the state transition to verify the proposed state before signing it and sending their signature to all other parties.

Channel Disputes/Closure. If an honest party does not receive n signatures before a local timeout, it assumes that there has been a disagreement about the proposed state. The honest party may trigger a layer-one *dispute* and enforce a new state transition without the cooperation of the other parties.

We generalize [28, 29] the properties and security guarantees for responsive parties offered by channels:

Unanimous Establishment: A channel is only considered open if all n parties agree to its establishment.

Unanimous Transition: A transition on layer-two, i.e. without an on-chain dispute, requires all n parties to agree.

Balance Security: An honest party can always withdraw the agreed balance from the channel with an on-chain dispute.

State Progression: A party can always enforce an off-chain state transition on-chain, the state machine thus always reaches a terminal state.

3.2 State Replacement Overview

Channel constructions are inherently based on state replacement techniques (cf. Figure 3). These techniques assume that participants in a channel are rational and follow the strategy with the highest payoff (e.g. a user publishes an older state if it represents a payment of higher value for this user). To be applicable for the wide range of protocols used to realize channels, the following section discusses generic state transitions. We distinguish four state replacement techniques:

[7] While the earliest channel protocols differ slightly from the above three-part *state replacement* technique, they nonetheless fit within the framework of unanimous consent coupled with the local verification of state transitions.

– *Replace by Incentive (RbI).* A sender shares newly authorized states with a receiver. A rational receiver only signs and publishes the state that pays the highest amount.
– *Replace by Time Lock (RbT).* Every state is associated with a time lock[8], which decrements every time the state changes. The state with the lowest time lock is considered the latest state, as it can be accepted into the blockchain before all previously authorized states. Once a channel closes, the state that is included in the blockchain deprecates all other states.
– *Replace by Revocation (RbR).* All parties collectively authorize a new state before revoking the previous state. Upon dispute, the blockchain provides a time period for parties to prove that the published state is a revoked state.
– *Replace by Version (RbV).* States have a monotonic increasing counter representing the state version. Upon dispute, the authorized state with the highest state version is considered the latest state. A new state replaces a previous state if it has a larger version number.

We provide further detail on the evolution of payment and state channels in Appendix A. For *RbI* and *RbT*, the latest state can only be written to the blockchain once. *RbR* and *RbV* introduce a dispute process where the counterparty can provide evidence that a state submitted to the blockchain is invalid. After the dispute, the off-chain contract can either be re-deployed to the blockchain (i.e. *closure dispute*, cf. Section A.2) or a set of commands can be executed via the blockchain (i.e. *command dispute*, cf. Section A.2). The introduction of a dispute process introduces a new assumption critical to the channel's security; the *always online assumption* [68] (cf. Section 8). Watching services mitigate the assumption by allowing users to delegate their responsibility of raising disputes to a third party.

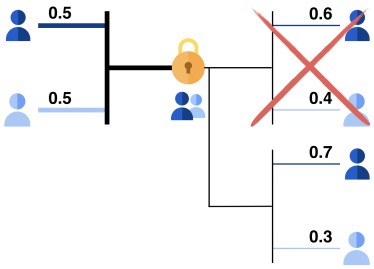

Fig. 3. Payment channel update (UTXO model), invalidate outdated state.

3.3 Watching Services

To alleviate the online assumption for channel users, related work proposes to outsource the responsibility of issuing challenges to third-party watching services [68–70]. Users outsource their latest state to the watching service before parting offline. Watching services then act on behalf of the users to secure their funds. Users can still verify the correct behavior of watching services and punish them (e.g. by keeping pre-allocated collateral) in case of non-compliance. Monitor [69] provides watching services within the Lightning Network. WatchTower [70] is designed for Eltoo and requires $O(1)$ storage but is currently not

[8] Time locks define either *absolute* time expressed as a blockchain block height, or *relative* time expressed as the number of blocks that must elapse after a transaction is included in the blockchain.

compatible with Bitcoin's consensus rules. PISA [68] provides watching services for state channels and requires $O(1)$ storage. PISA instances provide receipts to offline users; the users can burn an instance's security deposit if the instance misbehaves.

DCWC [71] enables users to engage with multiple watching services, increasing the probability of at least one honest watcher protecting the offline user's interests. On the other hand, Brick [72] proposes an additional proactive role for a watching service. Watchtower committees are formed to manage dispute resolution on behalf of channel participants (i.e. as opposed to executing the dispute process on the blockchain). This approach ensures channel participants are protected against blockchain latency and high transaction fees as the committee will decide the final agreed state for the channel and post it to the blockchain at a later time, but like PISA, its security relies on financial incentives and collateral lockup by members of the watchtower committee.

Outpost [73] achieves O(1) storage for a watchtower in Bitcoin without the need to change any consensus rules. Instead of sending an encrypted justice transaction to the watchtower for every update in the channel, the encrypted justice transaction is stored in the corresponding channel state (as an OP_RETURN). When there is a dispute in the channel, the encrypted justice transaction is recorded in the blockchain. Thus an observer with the decryption key can simply decrypt the justice transaction and relay it to the network. Cerberus [74] considers how to build financially accountable watchtowers in Bitcoin (as PISA accomplished in Ethereum). It requires the watchtower to lock up collateral for each channel it is watching and to participate in every channel update. If the watchtower fails to protect the channel participants, then the participants can force the watchtower to forfeit its deposit.

3.4 Channel Hierarchy

Aiming to reduce the number of required on-chain transactions, there have been proposals to increase the flexibility of channels with regard to applications and participants.

Multiple Applications. Dziembowski *et al.* [75] and Counterfactual [76] explore the possibility of installing and uninstalling applications off-chain (i.e. without on-chain fee) [9]. This allows parties to execute multiple concurrent applications (e.g. tic-tac-toe, poker and bi-directional payments). Such modular channels maintain a set of application instances and each instance operates on an individually allocated collateral. Application instances are isolated from each other (even in case of disputes) and based on *RbV*. Collateral is unanimously assigned to one application and cannot be used simultaneously for other applications due to security reasons.

Channel Factories. Burchert *et al.* [37] propose the concept of a channel factory for Bitcoin, whereby n parties lock coins into a n-party deposit that is then

[9] See A.2 for detail on the notions of *installing* and *uninstalling* in this context.

re-allocated to a set of pair-wise payment channels. Each party may maintain one or more pair-wise channels to facilitate transactions. Whenever two parties want to establish a direct channel, all parties cooperatively agree to create a new re-allocation of pair-wise payment channels by jointly updating the n-party deposit. This re-allocation of pair-wise channels can be built using DMC [37], while Ranchal-Pedrosa *et al.* [77] replace DMC with Lightning channels.

3.5 Channel Synchronization

The channel designs discussed in the previous section are limited to the direct interaction among connected parties. This brings forth a new question of whether it is possible for two (or more parties) to avoid setting up a new direct channel on the parent blockchain (and thus avoid prohibitive fees) by finding a path of separate existing channels that indirectly connects them on the network. For instance, if Alice has a channel with Bob, and Bob has a channel with Caroline, then Alice could transact with Caroline via Bob. Such a network of channels is known as a Payment Channel Network (PCN). To facilitate synchronizing a payment (or executing a smart contract) across a path of channels, we present *conditional transfers*. Those allow the sender to lock coins into a transfer such that the receiver can only claim the funds if a condition is satisfied before an expiry time [78–81]. Channel synchronization requires every hop along the path to set up conditional transfers with their counterparty. Two security properties are crucial for channel synchronization. First, *no counterparty risk* is required to ensure that no party defaults on its obligation to execute a transaction in the prescribed manner. Second, *atomicity* ensures that a transaction either succeeds or fails in its entirety. Atomicity is particularly important if one transaction is split over multiple payments or paths. We provide further detail on techniques for channel synchronization in Appendix B.

Virtual channels. In all constructions discussed previously, intermediate users are required to remain online and explicitly confirm all mediated transactions to successfully synchronize their channels. Dziembowski et al. [29,75] address these shortcomings with the introduction of virtual channels that support payment and state transitions. All intermediaries along the route can lock coins for a fixed period of time and both parties can treat the path as a new *virtual channel* connecting them directly. In this manner, A and B can transact without interacting with intermediaries along the path, thus reducing the transaction latency. Virtual channels are limited by the need to recursively set up a new virtual channel for every intermediary along the path. It is the intermediary's responsibility to ensure the channels close appropriately. Dziembowski et al. [82] extended virtual channels to support more than two parties such that any number of parties can set up a virtual channel without blockchain interaction.

3.6 Routing

If A wants to pay B using a set of intermediate channels, it is necessary to first find one or several paths of open channels from A to B. If the payment only

utilizes a single path, all channels need to have sufficient collateral to conduct the payment. If the payment is split over multiple paths, it is necessary to divide the payment in such a manner that channels on each path can handle the partial payment. In this section, we introduce *routing algorithms*, i.e. algorithms for finding paths in a network of payment or state channels. For simplicity, we use the example of payment channels throughout the section. The protocols, however, do apply to state channels.

Existing network routing algorithms for data transmission experience unique challenges when applied to PCNs. The goal of data routing algorithms is the transfer of data from one node to another, i.e. routing changes the state of nodes by transferring information. Node links and bandwidth capacities in data networks moreover are not considered private information. Retransmission of data is an inherent feature of e.g. TCP, and typically doesn't induce significant economic losses to either sender or receiver.

In contrast, the goal of a payment channel routing algorithm is to change the state of the traversed channels to secure the asset delivery from sender to receiver. Depending on the transaction amount, certain channels may not be suitable to route a payment, and channel balances are thus an obstacle that routing algorithms have to account for. An executed channel transaction permanently alters the state of all channels along the path. Further parameters, such as bandwidth and network latencies moreover influence channel path delay characteristics. To protect user privacy, only the total capacity of a channel is disclosed, not the distribution of funds among the two channel participants. Channel transactions might therefore fail and the routing algorithms attempt different execution paths until one succeeds. PCN routing algorithms, therefore, have to account for the unique characteristic of channels to provide satisfactory path recommendations[10]. We summarize five crucial properties routing algorithms for payment channels should satisfy [30–32].

Effectiveness: Given a PCN snapshot and the channel balances, the algorithm should find paths which maximize the success probability of a payment. The algorithm should remain effective when channel balances change.

Efficiency: The overhead of path discovery should be low in latency, communication and computation. Changes of the PCN topology should entail a low update overhead cost.

Scalability: The routing algorithm should remain effective and efficient for large-scale PCNs and high transaction rates.

Cost-Effectiveness: The algorithm should find paths with low transaction fees. The fees of a layer-two transaction should be lower than a layer-one transaction.

Privacy: Routing paths should be found without disclosing transaction values (i.e. value privacy) and the involved parties (i.e. sender and receiver privacy).

We distinguish between two classes of routing algorithms: global routing and local routing. In global, or source routing, each node maintains a local snapshot

[10] Note that Tor-like routing is inappropriate, as Tor assumes a random relay selection, which wouldn't account for channel capacities.

of the complete PCN topology. In local routing, the algorithm operates on local information, i.e. is only aware of the node neighbors with which it established channels with. We summarize the performance of algorithms presented in related work in Appendix G Table A2 and provide further detail on routing algorithms in Appendix C.

3.7 Payment Channel Hubs

Related work [83] observes that layer-two systems benefit from centralized (but non-custodial) star-topologies to reduce *(i)* collateral lockup costs and to *(ii)* simplify routing complexities. A payment channel hub (PCH) is essentially a node in a PCN that maintains many channels with different peers. Having a network with multiple interconnected PCHs should result in a lower average path length. A reduced path length implies a reduction in collateral cost and route discovery complexity. Still PCHs face significant locked capital requirements for each channel. For example, a PCN node with $1M$ channels, each channel sending on average \$1000 of transaction volume, requires the hub to lock up a total of $\$1B$. Rebalancing operations are only possible via costly and slow parent-chain transactions. Moreover, user-onboarding is a costly process, a PCN node with $1M$ users would require $1M$ parent-chain setup transactions (costing more than $\$100k$ on Ethereum).

3.8 Summary

In this section we have presented the evolution of channel constructions from *Replace by Incentive* through to *Replace by Version*. Given a network of channels, we have considered the role of conditional transfers to let parties synchronize payments (or construct new virtual channels) across a path of channels. With respect to routing and finding a path that connects two parties in a channel-based network, we discussed the limitations of deployed routing algorithms due to their reliance on source routing. Alternative algorithms that rely only on local knowledge offer some promise, but require further work to achieve effectiveness comparable to that of source routing. Finally a significant consequence of channel networks is the requirement for users to remain online and synchronized with the network to watch for malice disputes. To alleviate the online assumption, there are several proposals for third party watching services who can respond to a dispute on the user's behalf. All proposals tend to focus on building highly available watching networks and using on-chain collateral to ensure the watching services can be held financially accountable.

The aforementioned results suggest that blockchains can scale further by leveraging layer-two technologies and thus without changes to the underlying layer one. However, PCNs experience limitations and their scalability properties have not yet been quantified appropriately. While layer-one transaction costs are quantified by their *size* (on UTXO blockchains), or computational complexity (on smart contract blockchains), the transaction costs on layer-two are primarily correlated to the transaction value (in \$). The higher a layer-two transaction value, the more on-chain collateral needs to be reserved, locking up potentially

considerable amounts of funds *in advance*. Analysis of the economic consequences of channel constructions, (e.g. as conducted in [84]), is an open and important area for future work, particularly in relation to the economic incentives for channel watching services [85] and the fee structures for channel payments [86].

4 Commit-chains

In this section we provide an overview of commit-chains. We provide detail in Appendix D, in particular describing two pioneering commit-chains proposals: NOCUST [26] (section D.1), an account-based commit-chain, and Plasma [38] (section D.2), a UTXO-based commit-chain. In Appendix G Table A3, we provide an overview of the properties of NOCUST and Plasma Cash [87] (a simplified Plasma variant).

4.1 Commit-chain Overview

In contrast to channels, commit-chains are maintained by one single party that acts as an untrusted intermediary for managing transactions between users. Hence, commit-chains serve a similar purpose as payment channel hubs but with protocols specifically optimized for this scenario. The operator is responsible for collecting commit-chain transactions from the users and periodically submits a commitment to all collected transactions to the parent-blockchain. Unlike channels, commit-chains do not rely on a three-state model (opening, transitions, dispute/closure phase), but rather on an *always ongoing state* once launched. After an operator has launched a commit-chain, users can join by contacting the operator. They can then conduct transactions that are recorded on the commit-chain. Users can anytime withdraw or move their assets to the parent chain.

Periodic Checkpoint Commitments. Commit-chain users may need to periodically return online to observe the on-chain checkpoint commitment, which can be instantiated as a Merkle tree root or a Zero Knowledge Proof (ZKP) [26, 88]. Merkle root commitments do not self-enforce valid state transitions and therefore require users to participate in challenge-response protocols if a commitment is invalid. In contrast, ZKPs enforce consistent state transitions on-chain, thus reducing potential operator misbehavior. A challenge response mechanism is still required to ensure the completeness of the checkpoint (i.e., that it summarizes the latest state of all user accounts). Currently, there exists no efficient method to instantiate commit-chains on blockchains without highly expressive scripting languages.

Data Availability. As commit-chain data is not broadcast for efficiency reasons, users must retrieve/maintain data required to (partially) exit a commit-chain, commonly referred to as the data availability requirement. Data availability challenges may challenge a commit-chain operator to provide the necessary data or halt the operator upon misbehavior [26], allowing users to exit with their last confirmed balance.

Centralized but Untrusted Intermediary. The centralized operator may become a point of availability failure, but it does not hold custody of funds. The

operator may thus censor commit-chain transactions, encouraging mistreated users to exit anytime and move towards another commit-chain.

Eventual Transaction Finality. Unlike previously discussed layer-two protocols, the intermediary commit-chain operator does not require on-chain collateral to securely route a payment between two commit-chain users. In this setting, commit-chain transactions do not offer instant transaction finality (as in channels), but eventual finality after commit-chain transactions are recorded securely in an on-chain checkpoint.

Reduced Routing Requirements. Because a commit-chain can potentially host millions of users, few statically connected commit-chains are envisioned to spawn stable networks with low routing complexity. However, we are not aware of any proposals for atomic cross commit-chain transactions.

We generalize the security properties for users as follows:

Free Establishment: Users join a commit-chain without an on-chain transaction by requesting an operator signature [26].
Agreed Transition: A commit-chain transaction is agreed upon by at least the sender and the commit-chain operator.
Balance Security: Honest users can always withdraw agreed balances from the commit-chain with an on-chain dispute.
State Progression: User can enforce an off-chain state transition on-chain.
Commitment Integrity: Users can verify the integrity of commitments and force the commit-chain operator to seize operation (and rollback to the latest commitment)[11].

Unlike with channels, *state progression* is not a default security property for commit-chains, because they only offer *eventual finality*, unless off-chain transactions are secured by additional collateral [26]. In the worst case, transactions remain unconfirmed if the next commitment is invalid or not provided.

4.2 Summary

Unlike channels, commit-chains allow transaction recipients to remain offline at the time of payment, approaching similar usability properties to layer-one transactions. Conditional on using smart contract enabled blockchains, commit-chains also allow for a reduction in the required layer-two collateral.

Commit-chains have been shown to scale PoW blockchains by several orders of magnitude [26], trading-off decentralization for a more centralized (but non-custodial) architecture. Due to periodic checkpoints in commit-chains, delayed transaction finality is secure without collateral of the intermediate operator [26]. Operator collateral is "re-usable" [26] after each checkpoint, potentially reducing the locked capital and on-chain costs of PCHs.

[11] To mitigate the possibility of a false accusation attack by a user against the operator, the operator may require the user to subsidize the cost of a response to such a challenge. Note that this in turn may introduce a user grieving vector. To date, no appropriate parameterization or more elegant solution has been proposed.

Table 1 provides an overview and comparison of channel, channel-hub and commit-chain constructions.

Table 1. Comparison of layer-two transaction designs[1].

	Channel	Channel Hub	Commit-Chain
Topology	Mesh	Star	Star
Lifecycle	3-phase	3-phase	Periodic commit
Compatibility	Any chain	Any chain	Smart Contract chain
Privacy	value privacy, relationship anonymity	payment anonymity, unlinkability	✕
Offline TX Reception	✕	✕	✓
Mass-Exit Security	✕	✕	✓(payments)
TX Finality	Instant	Instant	Delayed or Instant
Instant TX Collateral	Full	Full	Reusable [26]
Delayed TX Collateral	NA	NA	0
Collateral Allocation	$O(n)$ on-chain	$O(n)$ on-chain	$O(1)$ on-chain [26]
User On-Boarding	On-chain TX	On-chain TX	Off-chain [26]

[1] Protocols for refereed delegation, distinct in nature with less focus on payments, are presented in Section 5.

5 Protocols for Refereed Delegation

In this section, we overview the protocols that focus on solving disputes among participants differently to how they are handled in channels and commit-chains[12].

So far we have assumed that all state transitions in an off-chain protocol can be executed on a layer-one blockchain. Such transitions range from the execution of conditional transfers to the execution of an application for a state channel. Yet while the layer-two approaches we have considered so far allow us to significantly increase the number of state updates performed among two or more parties, they are restricted to those whose dispute resolution mechanism builds upon a mechanism that can be *fully* executed on-chain. We now present two approaches which seek to reduce the on-chain requirements for the dispute resolution, thereby enlarging the set of feasible layer-two applications.

5.1 Bi-section Protocols

Instead of forcing conflicting users to post their (partial) state on-chain, a bi-section protocol works in two stages: (i) users look for the minimal verification step required to convince a third party (e.g., miner) of the validity of their statement; (ii) miners verify the (simplified) state from conflicting users to determine who is right. Truebit [45] and Arbitrum [44] are two approaches in this paradigm.

Truebit [45], inspired by verifiable computation, proposed the use of bi-section protocols to extend the computational capacity of a layer-one blockchain by taking the computation off-chain. At a high level, for a given computational task, a *solver* will post the solution alongside a commitment to a list of sub-tasks

[12] In contrast to channels, commit-chains have not yet been specified to support arbitrary state transitions.

that led to the solution. The blockchain enforces a challenge period to let challengers verify the solution's correctness off-chain and issue a challenge if they disagree. If there is a disagreement, the blockchain enforces a verification game that performs a binary-search for the list of sub-tasks. When it finds the task that led to the disagreement, it will simply execute it on-chain and verify the claim. While the above approach permits scalable off-chain computation, every verification game requires a logarithmic number of transactions depending on the size of the computation.

Arbitrum [44] takes this approach further by introducing a new virtual machine and a state channel. This lets a distributed set of parties execute a program in a custom virtual machine and unanimously agree to a commitment (i.e. state assertion) of the program's new state. If co-operation in the state channel breaks down, then any party in the channel can compute a state transition and post a commitment to the new state to the blockchain (i.e. a disputable assertion). This triggers a similar dispute process to that used in Truebit, where any other party can challenge the assertion and participate in a bi-section protocol.

6 Complementary Approaches For Layer-two Protocols

In this section we present two sets of approaches which are complementary to layer-two protocols: (i) trusted execution environments and (ii) side-chains. In contrast to layer-two protocols, these approaches invoke additional and differentiated trust assumptions. Trusted execution environments require a shifted trust assumption towards the CPU manufacturer. Side-chains require trust in the independent consensus algorithm of the side-chain.

6.1 Trusted Execution Environments

The trusted execution environment (TEE), e.g. Intel SGX [89], approach constitutes an orthogonal approach to that of existing layer-two protocols and can provide a high level of efficiency while requiring a benign hardware manufacturer.

Trusting a TEE to provide integrity naturally overcomes many obstacles of non-TEE protocols:

No collateral lockup: TEEs absorb the trust requirements, otherwise guaranteed via on-chain collateral.

Interoperability: The computation at the TEE can encode the logic and transaction format required for any blockchain.

Parallelized Disputes: TEEs can emulate the logic of global preimage manager to enable parallel disputes [13].

Ensured fees: TEEs follow the protocol definitions and pay honest users for their synchronization service.

Note that besides the shifted trust assumptions towards the CPU manufacturer, TEEs suffer from their own security concerns such as rollback [51] and side-channel attacks [90].

[13] For detail on global preimage manager see Appendix B.

Teechain [47] and Teechan [48] synchronize payments across channels using TEEs. TEE enable expressive and off-chain smart contracts on restricted Bitcoin-based blockchain [49]. Tesseract [91] proposes to construct a scalable TEE based real-time cross-chain cryptocurrency exchange. In relation to light clients in Bitcoin, BITE [92] leverages TEEs to enable full nodes to serve privacy-preserving requests from light clients, when used in combination with other private information retrieval and side-channel protection techniques. ZLiTE [93] also leverages TEEs to provide privacy-preserving light clients for Zcash, whereby light clients operate in conjunction with a TEE-enabled server (e.g., running Intel SGX [89]).

6.2 Side-chains

A second complementary approach is that of side-chains [19]. A side-chain is a distinct blockchain with a separate consensus algorithm attached to a parent-chain. Side-chains validate transactions and hence take over some of the parent-chain's load. Side-chains enable digital assets to be moved between a parent-chain and a side-chain, such that alternative blockchains can be developed without necessitating the creation of an alternative digital asset or coin: the parent-chain asset can be used directly on the side-chain.

The central innovation for side-chains is that of a two-way peg. A two-way peg is the mechanism permitting the transfer of digital assets at a certain exchange rate between a parent-chain and a side-chain. A two-way peg allows digital assets to be transferred from a parent-chain to a side-chain by sending parent-chain coins an output on the parent-chain that is locked by a Simplified Payment Verification (SPV) proof [19], which can then be unlocked by an SPV proof on the side-chain. For the period in which digital assets are locked on the parent-chain, the assets can be moved freely around on the side-chain. To transfer assets back to the parent-chain, funds are sent to an SPV locked output on the side-chain and an SPV proof on the parent-chain unlocks previously locked funds on the parent-chain. The varieties of a two-way peg are as follows.

Symmetric: SPV security is required to transfer funds between the side-chain and the parent-chain, independently of the direction.

Asymmetric: where users of the side-chain are fully aware of the state of the parent-chain, such that an SPV proofs are not required to transfer funds from a parent-chain to a side-chain, but are required to transfer funds back.

Side-chain constructions treat assets from different parent-chains as different asset types, which are not interchangeable but which can be explicitly traded. Potential limitations to the use of side-chains [19] include, for instance, an increase in complexity at both the network and asset level, the creation of new attack vectors, and an increase in the risks associated with centralized mining.

7 Anonymity and Privacy

In this section we first set out the relevant privacy concepts for layer-two (section 7.1), before exposing privacy enhancing protocols (section 7.2).

Layer-one transaction anonymity and privacy is extensively studied [94–97], uncovering that blockchain pseudonymity does not entail strong privacy guarantees. A public blockchain allows an adversary to link a sender and receiver of payments as well as trace back the origin of coins, breaking the *unlinkability* and *untraceability* properties. Privacy-focused blockchains [98–101] build upon cryptographic techniques [102–104] to obfuscate on-chain information. Unfortunately, side-channel information (e.g. usage patterns) enable linkability and traceability attacks [98, 105–108]. As off-chain transactions only have a minimal blockchain footprint, one might believe they provide privacy-by-design.

However, achieving privacy and unlinkability of layer-two transactions is not trivial [41, 78, 109]. The creation of a channel associates a permanent pseudonym (e.g. public keys), while synchronization among channels (cf. Section 3.6) may reveal the pseudonym of the cooperating parties. In Lightning, the a node ID is linked with an IP address and this information is broadcast across the network. Furthermore, naive route discovery among two channels with a disjoint set of participants might require the knowledge of the (partial) topology for the channel network. In HTLC payments (cf. Section 3.5), the intermediate channels on the path use the same cryptographic condition $y = H(R)$. An adversary on the path can observe the channel updates (i.e. share the same condition y) and can deduce who is paying to whom.

7.1 Layer-Two Privacy Notions

We differentiate between *(i)* an *off-path* adversary, which only has access to the blockchain; and *(ii)* an *on-path* adversary, which additionally participates in the layer-two protocol.

Payment Hub Privacy A PCH (cf. Section 3.7) or commit-chain (cf. Section 4) operator may have access to mediated transaction amounts and sender or receiver pseudonyms. In this setting, we consider the following privacy notions.

Payment Anonymity [41]: In the absence of side channels, the receiver of a payment, possibly in collusion with a set of malicious senders, learns nothing about an honest sender's spending pattern.

Unlinkability [39]: The operator cannot link the sender and the receiver of a given payment among the set of all feasible sender-receiver pairs.

Multi-Hop Privacy We consider the following privacy properties for routed payments (cf. Section 3.6).

(Off-path) Value Privacy [78]: An adversary not involved in a payment does not learn the transacted value. If the adversary is part of the payment path it trivially learns the transacted value while forwarding it.

(On-path) Relationship Anonymity [78]: Given two payments between two pairs of honest sender and receiver, the adversary (who might control some of the intermediate channels) cannot tell which sender paid to which receiver with a probability higher than 50%. Off-path adversaries are not considered here since transaction data is shared only among involved participants.

Unlike other payment networks such as credit networks [30,110–112], existing privacy notions in PCNs do not consider link privacy (e.g. whether an adversary can determine the existence of a payment channel between two users) or whether it is possible to infer the (partial) topology of a PCN. Channels may be unannounced (e.g. private Lightning channels), such that an adversary may be unaware of the link between users.

7.2 Privacy Enhancing Protocols

While related work covers layer-one transaction privacy extensively [99,113–120], it is as yet unclear if such techniques are applicable to layer-two protocols. Instead, the literature proposes layer-two tailored privacy proposals. We distinguish among *(i)* hub-based and *(ii)* multi-hop payment protocols.

Privacy Enhancing Payment Channel Hubs

TumbleBit. TumbleBit [39] is a unidirectional PCH relying on an untrusted intermediary, a *Tumbler*. The Tumbler issues anonymous vouchers that users can exchange for coins. A key aim of TumbleBit is to prevent an adversary from linking a payment from a particular payer to a particular payee (an unlinkable payment hub). Recent work (A2L) [81] improves the interoperability and efficiency of TumbleBit while preserving the security and privacy notions of interest. However, in both TumbleBit and A2L, the collusion between the Tumbler and the payee in combination with timing analysis can considerably reduce the number of potential payers. Similarly, side channels (e.g. a unique product price) allow the set of feasible sender-privacy pairs to be narrowed. Particular threats that are not addressed by the current design are: *(i) intersection attacks* [121] correlate information across different time periods, *(ii) abort attacks* gain information about other parties through abort of transactions, and *(iii)* $n-1$ *attacks* where the tumbler refuses all but one payment.

Bolt. Bolt [41] aims to offer privacy-preserving payment channels such that multiple payments on a single channel are unlinkable to each other. Assuming the channels are indeed funded with anonymized capital (e.g. using anonymized assets [99]), Bolt payments are anonymous.

Privacy Enhancing Multi-Hop Payment Protocols

Rayo and Fulgor [78]. : *Unlinkable Hashed Time-Locked Contract (HTLC)* [78][14], is a cryptographic primitive that ensures that a HTLC in a payment path is built upon a different and unrelated hash value. Each intermediate user is provided with two hash values $y_i := H(x_i)$ and $y_{i+1} := H(x_i \oplus x_{i+1})$ and the value x_{i+1}. The intermediate user is also provided with a ZKP that the preimage of y_{i+1} is the same as the one of y_i, just skewed by the value x_{i+1}. Rayo and Fulgor achieve the same functionality as HTLC but prevent linkability of payments.

[14] See Appendix B for detail on HTLCs.

Anonymous MHL (AMHL). Unlike Rayo and Fulgor, AMHL protocol embeds the synchronization condition within a public key, improving upon Rayo and Fulgor on efficiency and privacy (i.e. the synchronization condition does not explictly appear on the transaction).

Z-channel [122]. is a channel construction for Zcash [123], seeking to provide a payment channel construction leveraging the cryptographic schemes (and thus privacy properties) of Zcash. In particular, Z-Channel defines an extension of the distributed anonymous payment scheme (i.e., the payment scheme of Zcash) that integrates multisignature and time lock functionalities. Building upon this extension, Z-Channel conceptually mimics bidirectional micropayment channels as implemented in Bitcoin but using Zcash as the underlying blockchain.

7.3 Summary

We have seen that while the default transaction privacy on layer-two is likely better than on layer-one, layer-two transactions cannot by default be considered private. TumbleBit and A2L achieve unlinkability but not payment anonymity. BOLT does not support Bitcoin but offers stronger privacy guarantees. Even in the simplified PCH setting, it seems that tradeoffs between privacy and compatibility are required. Multi-hop payment protocols do not enforce single hop privacy guarantees (e.g a user learns predecessor and successor in a payment path) at the gain of global privacy guarantees such as value privacy and relationship anonymity. As demonstrated in AMHL, it is possible to achieve privacy guarantees and backwards compatibility with most existing blockchains. State channels and commit-chains demonstrate interesting functionalities based on the expressiveness of rich scripting languages. These protocols, however, to date do not aim at providing anonymity and privacy guarantees from the commit-chain operator. Instead, privacy is considered an orthogonal research problem. Recent work [44, 45] demonstrates that including additional verification functionality to the consensus layer opens the door for hiding contract activity in state channels.

8 Security

This section provides an overview of layer-two security concepts.

The consensus [1, 124] and network [125] security of blockchains has been extensively investigated. Security is fundamental to distributed ledgers, as the shift of trust assumptions from a single custodian to a decentralized non-custodial network only prevents the loss of funds if the system's security properties are sound. Layer-two research benefits from this body of literature, but necessitates the introduction of new requirements, trust assumptions and adversarial models.

8.1 Layer-Two Security Notions

While experimental studies so far focus on the connectivity of PCNs [126], formal security studies focus on the notion of *balance security*, both in the payment hub [39, 41] and multi-hop payment [78] settings, as well as provably secure off-chain protocols for multi-party computation [127]. Balance security intuitively

defines that layer-two protocols must achieve two properties: (i) the adversary cannot extract more funds than previously allocated in the channel's funding; (ii) honest users do not lose funds even when other parties collude. As with privacy, this security concept has been formalized in both paradigms: cryptographic games and the UC framework. BOLT, A2L and TumbleBit are the payment hub systems with formal security guarantees, while Rayo & Fulgor, AMHL and Perun provide formal security guarantees in the multi-hop setting. While previous work assumes a somewhat ideal model for the underlying blockchain to highlight the security and privacy properties at layer-two, recent work [128] shows a security analysis of the Lighting Network, tracing how its security properties build upon a blockchain model that faithfully represents Bitcoin at present. However, the work [128] does not model aspects such as fees, privacy, or cooperative channel closure. NOCUST provides a thorough study of *balance security* for commit-chains.

Consistency Proofs. Many layer-two protocols rely on challenge-response protocols to detect and prove misbehavior using the blockchain as a recourse for disputes. An alternative strategy to enforce consistency of an off-chain protocol is to let the blockchain verify a succinct proof attesting to consistency of the second layer's state. While ZKPs [129] suffer from expensive on-chain verification costs (approximately 650k gas on Ethereum) per proof [130], they can attest to potentially large state transitions which otherwise would require significant on-chain resources. For commit-chains, zkSNARKS were shown to enforce consistent checkpoints [26], leaving data availability of the external ledger as the remaining challenge vector.

8.2 Layer-Two Security Threats

There are security threats idiosyncratic to layer-two, detailed in Appendix E, as follows.

Hot Wallets: Channels' requirement of unanimous agreement for state updates, and therefore that all involved parties need to be online with access to their signing keys, makes it critical to keep keys online in a *hot wallet*. These wallets make parties prime targets for adversaries.

Online Assumption: Parties are required to remain online and fully synchronized with the PCN and blockchain. Therefore if a party goes offline, they become vulnerable to an adversary.

Blockchain Reliability and Mass Exits: Layer-two designs assume that the underlying blockchain accepts transactions eventually; however, under congestion, parties may fail to meet deadlines to settle disputes.

Security of Synchronizing Protocols: such as the *wormhole attack* [79], where transaction fees can be stolen, and the *American Call Option Attack* [131], where an adversary sets up a multi-hop payment but does not release the trigger to finalize the payment.

8.3 Summary

The security guarantees of layer-two transactions rely not only on the parent chain's consensus guarantees and on-chain security collateral data availability concerns and blockchain congestion threats introduce a new dimension of game-theoretic challenges that are not considered by current formal definitions. For instance, current UC definitions consider the blockchain as ideal components, which disregards the mass-exit concern.

9 Conclusion

This SoK systematizes the rich literature that has emerged on layer-two transactions since the inception of cryptocurrencies in 2009, categorizing the work into three main approaches: payment and state channels, commit-chains and protocols for refereed delegation. In addition to presenting the central aspect of the protocols in these three categories, we review in detail their anonymity, privacy and security aspects. Our over-arching aim in this paper is to lower the *barrier to entry* to the study of layer-two protocols.

We observe, overall, that layer-two protocols enable blockchains to scale without modification on the base layer but that the performance improvement results in different security guarantees for off-chain payments than on-chain transactions. We also observe a likely inherent trade-off between collateral and transaction finality at layer-two. In the context of channel constructions, instant finality requires full collateralization. For commit-chains, the requirements for full on-chain collateralization is reduced but in exchange for eventual finality. Notably, commit-chains enable secure off-chain transactions without collateralizing the full off-chain transaction volume. We present a series of open challenges for layer-two blockchain protocols in Appendix F.

Both payment channels and commit-chains face privacy challenges. Our discussion highlights clearly that not publishing transactions on a public blockchain is not sufficient for solving the privacy issues experienced in blockchain systems. Privacy in off-chain transactions requires common definitions and new protocols.

We explicitly lay out the shift in transaction costs from transaction size (in bytes) to transaction value. It stands to reason that such a shift entails economic consequences. In particular, the relation between on-chain and off-chain fees raises interesting game-theoretical questions for a rational actor aiming to minimize the fees they pay or maximize the fees they gain.

Acknowledgments The authors would like to thank Alexei Zamyatin and Sam Werner for their valuable feedback on earlier paper versions. This work has been partially supported by the Austrian Research Promotion Agency through the Bridge-1 project PR4DLT (grant agreement 1380869); by EPSRC Standard Research Studentship (DTP) (EP/R513052/1); by COMET K1 SBA, ABC; by Chaincode Labs; by the Austrian Science Fund (FWF) through the Lisa Meitner program; by the Ethereum Foundation, Ethereum Community Fund and Research Institute.

References

1. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: Conference on Computer and Communications Security. pp. 3–16. ACM (2016)
2. Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G., et al.: On scaling decentralized blockchains. In: International Conference on Financial Cryptography and Data Security. pp. 106–125. Springer (2016)
3. VISA: Visa inc. at a glance (2015), available at: `https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf`
4. Kiayias, A., Russell, A., David, B., Oliynykov, R.: Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Annual International Cryptology Conference. pp. 357–388. Springer (2017)
5. Buterin, V.: Slasher: A punitive proof-of-stake algorithm (2014), available at: `https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/`
6. Anon.: Casper (2018), available at: `https://github.com/ethereum/casper`
7. Miller, A., Juels, A., Shi, E., Parno, B., Katz, J.: Permacoin: Repurposing bitcoin work for data preservation. In: Symposium on Security and Privacy. pp. 475–490 (2014)
8. Hønsi, T.: Spacemint-a cryptocurrency based on proofs of space. IACR Cryptology ePrint Archive (2017)
9. Sawtooth (2019), available at: `https://intelledger.github.io/introduction.html`
10. Kogias, E.K., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., Ford, B.: Enhancing bitcoin security and performance with strong consistency via collective signing. In: USENIX Security Symposium. pp. 279–296 (2016)
11. Luu, L., Narayanan, V., Baweja, K., Zheng, C., Gilbert, S., Saxena, P.: Scp: A computationally-scalable byzantine consensus protocol for blockchains. IACR Cryptology ePrint Archive 2015, 1168 (2015)
12. Pass, R., Shi, E.: Hybrid consensus: Efficient consensus in the permissionless model. In: 31 International Symposium on Distributed Computing. p. 6 (2017)
13. Eyal, I., Gencer, A.E., Sirer, E.G., Van Renesse, R.: Bitcoin-ng: A scalable blockchain protocol. In: Symposium on Networked Systems Design and Implementation). pp. 45–59 (2016)
14. Anon.: Sharding roadmap (2019), available at: `https://github.com/ethereum/wiki/wiki/Sharding-roadmap`
15. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., Saxena, P.: A secure sharding protocol for open blockchains. In: Conference on Computer and Communications Security. pp. 17–30. ACM (2016)
16. Gencer, A.E., van Renesse, R., Sirer, E.G.: Service-oriented sharding with aspen. arXiv preprint arXiv:1611.06816 (2016)
17. Zamani, M., Movahedi, M., Raykova, M.: Rapidchain: Scaling blockchain via full sharding. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. pp. 931–948. ACM (2018)
18. Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., Ford, B.: Omniledger: A secure, scale-out, decentralized ledger via sharding. In: Symposium on Security and Privacy. pp. 583–598 (2018)

19. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P.: Enabling blockchain innovations with pegged sidechains. URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains (2014)
20. Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., Danezis, G.: Consensus in the age of blockchains. arXiv preprint arXiv:1711.03936 (2017)
21. Bitcoin cash (2008), available at: `https://www.bitcoincash.org`
22. Hearn, M.: Micro-payment channels implementation now in bitcoinj (2013), available at: `https://bitcointalk.org/index.php?topic=244656.0`
23. Anon.: bitcoinj (2019), available at: `https://bitcoinj.github.io/`
24. Decker, C., Wattenhofer, R.: A fast and scalable payment network with bitcoin duplex micropayment channels. In: Symposium on Self-Stabilizing Systems. pp. 3–18. Springer (2015)
25. Poon, J., Dryja, T.: The bitcoin lightning network: scalable off-chain instant payments (2016), available at: `https://lightning.network/lightning-network-paper.pdf`
26. Khalil, R., Gervais, A., Felley, G.: Nocust–a securely scalable commit-chain (2018), available at: `https://eprint.iacr.org/2018/642.pdf`
27. AG, B.T.: Raiden network (2019), available at: `https://raiden.network/`
28. Miller, A., Bentov, I., Kumaresan, R., McCorry, P.: Sprites: Payment channels that go faster than lightning. arXiv preprint arXiv:1702.05812 (2017)
29. Dziembowski, S., Eckey, L., Faust, S., Malinowski, D.: Perun: Virtual payment channels over cryptographic currencies. In: Symposium on Security and Privacy (2019)
30. Malavolta, G., Moreno-Sanchez, P., Kate, A., Maffei, M.: Silentwhispers: Enforcing security and privacy in credit networks. In: Network and Distributed System Security Symposium (2017)
31. Roos, S., Moreno-Sanchez, P., Kate, A., Goldberg, I.: Settling payments fast and private: Efficient decentralized routing for path-based transactions (2018)
32. Sivaraman, V., Venkatakrishnan, S.B., Alizadeh, M., Fanti, G., Viswanath, P.: Routing cryptocurrency with the spider network. arXiv preprint arXiv:1809.05088 (2018)
33. Sunshine, C.A.: Source routing in computer networks. SIGCOMM Computer Communication Review 7(1), 29–33 (1977)
34. Anon.: Lightning-onion (2018), available at: `https://github.com/lightningnetwork/lightning-onion`
35. Prihodko, P., Zhigulin, S., Sahno, M., Ostrovskiy, A., Osuntokun, O.: Flare: An approach to routing in lightning network (2016), available at: `https://bitfury.com/content/downloads/whitepaper_flare_an_approach_to_routing_in_lightning_network_7_7_2016.pdf`
36. Khalil, R., Gervais, A.: Revive: Rebalancing off-blockchain payment networks. In: Conference on Computer and Communications Security. pp. 439–453. ACM (2017)
37. Burchert, C., Decker, C., Wattenhofer, R.: Scalable funding of bitcoin micropayment channel networks. Royal Society open science 5(8), 180089 (2018)
38. Poon, J., Buterin, V.: Plasma: Scalable autonomous smart contracts (2017), available at: `https://plasma.io/plasma.pdf`
39. Heilman, E., Alshenibr, L., Baldimtsi, F., Scafuro, A., Goldberg, S.: Tumblebit: An untrusted bitcoin-compatible anonymous payment hub (2017)

40. Heilman, E., Lipmann, S., Goldberg, S.: The arwen trading protocols
41. Green, M., Miers, I.: Bolt: Anonymous payment channels for decentralized currencies. In: Conference on Computer and Communications Security. pp. 473–489. ACM (2017)
42. Heilman, E., Baldimtsi, F., Goldberg, S.: Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In: International Conference on Financial Cryptography and Data Security. pp. 43–60. Springer (2016)
43. Atlas, K.: The inevitability of privacy in lightning networks (2017), available at: https://www.kristovatlas.com/the-inevitability-of-privacy-in-lightning-networks/
44. Kalodner, H., Goldfeder, S., Chen, X., Weinberg, S.M., Felten, E.W.: Arbitrum: Scalable, private smart contracts. In: {USENIX} Security Symposium. pp. 1353–1370 (2018)
45. Teutsch, J., Reitwiessner, C.: A scalable verification solution for blockchains, https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf
46. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In: Symposium on Security and Privacy. pp. 104–121. IEEE (2015)
47. Lind, J., Eyal, I., Kelbert, F., Naor, O., Pietzuch, P., Sirer, E.G.: Teechain: Scalable blockchain payments using trusted execution environments. arXiv preprint arXiv:1707.05454 (2017)
48. Lind, J., Eyal, I., Pietzuch, P., Sirer, E.G.: Teechan: Payment channels using trusted execution environments. arXiv preprint arXiv:1612.07766 (2016)
49. Das, P., Eckey, L., Frassetto, T., Gens, D., Hostáková, K., Jauernig, P., Faust, S., Sadeghi, A.R.: Fastkitten: Practical smart contracts on bitcoin
50. Costan, V., Devadas, S.: Intel sgx explained. IACR Cryptology ePrint Archive 2016(086), 1–118 (2016)
51. Matetic, S., Ahmed, M., Kostiainen, K., Dhar, A., Sommer, D., Gervais, A., Juels, A., Capkun, S.: {ROTE}: Rollback protection for trusted execution. In: {USENIX} Security Symposium. pp. 1289–1306 (2017)
52. Neudecker, T., Hartenstein, H.: Network layer aspects of permissionless blockchains. IEEE Communications Surveys & Tutorials (2018)
53. Decker, C., Wattenhofer, R.: Information propagation in the bitcoin network. In: Conference on Peer-to-Peer Computing. pp. 1–10 (2013)
54. Klarman, U., Basu, S., Kuzmanovic, A., Sirer, E.G.: bloxroute: A scalable trustless blockchain distribution network (2018), available at: https://bloxroute.com/wp-content/uploads/2018/03/bloXroute-whitepaper.pdf
55. Gervais, A., Capkun, S., Karame, G.O., Gruber, D.: On the privacy provisions of bloom filters in lightweight bitcoin clients. In: Computer Security Applications Conference. pp. 326–335 (2014)
56. Bitcoin fibre (2019), available at: http://www.bitcoinfibre.org/
57. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008), available at: https://bitcoin.org/bitcoin.pdf
58. Sompolinsky, Y., Zohar, A.: Accelerating bitcoin's transaction processing. fast money grows on trees, not chains. IACR Cryptology ePrint Archive 2013(881) (2013)
59. Lerner, S.D.: Decor + hop: A scalable blockchain protocol, available at: https://scalingbitcoin.org/papers/DECOR-HOP.pdf
60. Sompolinsky, Y., Lewenberg, Y., Zohar, A.: Spectre: A fast and scalable cryptocurrency protocol. IACR Cryptology ePrint Archive 2016, 1159 (2016)

61. Zhang, F., Eyal, I., Escriva, R., Juels, A., Van Renesse, R.: {REM}: Resource-efficient mining for blockchains. In: {USENIX} Security Symposium. pp. 1427–1444 (2017)
62. David, B., Gaži, P., Kiayias, A., Russell, A.: Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In: Conference on the Theory and Applications of Cryptographic Techniques. pp. 66–98. Springer (2018)
63. Bentov, I., Pass, R., Shi, E.: Snow white: Provably secure proofs of stake. IACR Cryptology ePrint Archive 2016, 919 (2016)
64. Milutinovic, M., He, W., Wu, H., Kanwal, M.: Proof of luck: an efficient blockchain consensus protocol. In: Proceedings of the 1st Workshop on System Software for Trusted Execution. p. 2. ACM (2016)
65. Borge, M., Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Ford, B.: Proof-of-personhood: Redemocratizing permissionless cryptocurrencies. In: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 23–26. IEEE (2017)
66. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper 151, 1–32 (2014)
67. Plasma cash: Plasma with much less per-user data checking (2018), available at: `https://ethresear.ch/t/plasma-cash-plasma-with-much-less-per-user-data-checking/1298`
68. McCorry, P., Bakshi, S., Bentov, I., Miller, A., Meiklejohn, S.: Pisa: Arbitration outsourcing for state channels. IACR Cryptology ePrint Archive 2018, 582 (2018)
69. Dryja, T.: Unlinkable outsourced channel monitoring (2016), available at: `https://scalingbitcoin.org/transcript/milan2016/unlinkable-outsourced-channel-monitoring`
70. Osuntokun, O.: Hardening lightning, harder, better, faster stronger (2015), available at: `https://cyber.stanford.edu/sites/g/files/sbiybj9936/f/hardening_lightning_updated.pdf`
71. Avarikioti, G., Laufenberg, F., Sliwinski, J., Wang, Y., Wattenhofer, R.: Towards secure and efficient payment channels. arXiv preprint arXiv:1811.12740 (2018)
72. Avarikioti, G., Kogias, E.K., Wattenhofer, R.: Brick: Asynchronous state channels. arXiv preprint arXiv:1905.11360 (2019)
73. Khabbazian, M., Nadahalli, T., Wattenhofer, R.: Outpost: A responsive lightweight watchtower. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies. pp. 31–40. ACM (2019)
74. Avarikioti, G., Litos, O.S.T., Wattenhofer, R.: Cerberus channels: Incentivizing watchtowers for bitcoin. Financial Cryptography and Data Security (FC) (2020)
75. Dziembowski, S., Faust, S., Hostáková, K.: General state channel networks. In: Conference on Computer and Communications Security. pp. 949–966. ACM (2018)
76. Joleman, J., Horne, L., Xuanji, L.: Counterfactual: Generalized state channels (2018), available at: `https://l4.ventures/papers/statechannels.pdf`
77. Pedrosa, A.R., Potop-Butucaru, M., Tucci-Piergiovanni, S.: Lightning factories (2019)
78. Malavolta, G., Moreno-Sanchez, P., Kate, A., Maffei, M., Ravi, S.: Concurrency and privacy with payment-channel networks. In: Conference on Computer and Communications Security. pp. 455–471. CCS '17, ACM, New York, NY, USA (2017), `http://doi.acm.org/10.1145/3133956.3134096`
79. Malavolta, G., Moreno-Sanchez, P., Schneidewind, C., Kate, A., Maffei, M.: Anonymous multi-hop locks for blockchain scalability and interoperability. In: Network and Distributed System Security Symposium (2019)

80. Egger, C., Moreno-Sanchez, P., Maffei, M.: Atomic multi-channel updates with constant collateral in bitcoin-compatible payment-channel networks. In: CCS (2019)
81. Tairi, E., Moreno-Sanchez, P., Maffei, M.: A^{2}l: Anonymous atomic locks for scalability and interoperability in payment channel hubs. IACR Cryptology ePrint Archive 2019, 589 (2019), https://eprint.iacr.org/2019/589
82. Dziembowski, S., Eckey, L., Faust, S., Hesse, J., Hostáková, K.: Multi-party virtual state channels. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 625–656. Springer (2019)
83. Avarikioti, G., Janssen, G., Wang, Y., Wattenhofer, R.: Payment network design with fees. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology, pp. 76–84. Springer (2018)
84. Brânzei, S., Segal-Halevi, E., Zohar, A.: How to charge lightning. arXiv preprint arXiv:1712.10222 (2017)
85. Avarikioti, G., Laufenberg, F., Sliwinski, J., Wang, Y., Wattenhofer, R.: Incentivizing payment channel watchtowers (2018), available at: https://scalingbitcoin.org/transcript/tokyo2018/incentivizing-payment-channel-watchtowers
86. Di Stasi, G., Avallone, S., Canonico, R., Ventre, G.: Routing payments on the lightning network. In: 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). pp. 1161–1170. IEEE (2018)
87. Konstantopoulos, G.: Plasma cash: Towards more efficient plasma constructions (2019), available at: https://github.com/loomnetwork/plasma-paper/blob/master/plasma_cash.pdf
88. Merkle, R.C.: A digital signature based on a conventional encryption function. In: Conference on the theory and application of cryptographic techniques. pp. 369–378. Springer (1987)
89. Intel: Intel software guard extensions (intel sgx) (2019), available at: https://software.intel.com/en-us/sgx
90. Brasser, F., Müller, U., Dmitrienko, A., Kostiainen, K., Capkun, S., Sadeghi, A.R.: Software grand exposure:{SGX} cache attacks are practical. In: 11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17) (2017)
91. Bentov, I., Ji, Y., Zhang, F., Li, Y., Zhao, X., Breidenbach, L., Daian, P., Juels, A.: Tesseract: Real-time cryptocurrency exchange using trusted hardware. IACR Cryptology ePrint Archive 2017, 1153 (2017)
92. Matetic, S., Wüst, K., Schneider, M., Kostiainen, K., Karame, G., Capkun, S.: Bite: Bitcoin lightweight client privacy using trusted execution. IACR Cryptology ePrint Archive 2018, 803 (2018)
93. Wüst, K., Matetic, S., Schneider, M., Miers, I., Kostiainen, K., Capkun, S.: Zlite: Lightweight clients for shielded zcash transactions using trusted execution. In: International Conference on Financial Cryptography and Data Security. Springer (2019)
94. Karame, G.O., Androulaki, E., Roeschlin, M., Gervais, A., Čapkun, S.: Misbehavior in bitcoin: A study of double-spending and accountability. ACM Transactions on Information and System Security (TISSEC) 18(1), 2 (2015)
95. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in bitcoin. In: International Conference on Financial Cryptography and Data Security. pp. 34–51. Springer (2013)

96. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 conference on Internet measurement conference. pp. 127–140. ACM (2013)
97. Böhme, R., Christin, N., Edelman, B., Moore, T.: Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives 29(2), 213–38 (2015)
98. Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., Narayanan, A., et al.: An empirical analysis of traceability in the monero blockchain. Proceedings on Privacy Enhancing Technologies 2018(3), 143–163 (2018)
99. Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from bitcoin. In: Symposium on Security and Privacy. pp. 459–474. IEEE (2014)
100. Grin: minimal implementation of the mimblewimble protocol (2019), https://github.com/mimblewimble/grin
101. Beam: Scalable confidential cryptocurrency. a mimblewimble implementation (2019), https://github.com/BeamMW/beam
102. Courtois, N.T., Mercer, R.: Stealth address and key management techniques in blockchain systems. In: ICISSP. pp. 559–566 (2017)
103. Bender, A., Katz, J., Morselli, R.: Ring signatures: Stronger definitions, and constructions without random oracles. In: Theory of Cryptography Conference. pp. 60–79. Springer (2006)
104. Feige, U., Fiat, A., Shamir, A.: Zero-knowledge proofs of identity. Journal of cryptology 1(2), 77–94 (1988)
105. Kappos, G., Yousaf, H., Maller, M., Meiklejohn, S.: An empirical analysis of anonymity in zcash. In: USENIX Security Symposium. pp. 463–477 (2018)
106. Hinteregger, A., Haslhofer, B.: An empirical analysis of monero cross-chain traceability. CoRR abs/1812.02808 (2018), http://arxiv.org/abs/1812.02808
107. Kumar, A., Fischer, C., Tople, S., Saxena, P.: A traceability analysis of monero's blockchain. In: ESORICS. pp. 153–173 (2017)
108. Biryukov, A., Feher, D.: Privacy and linkability of mining in zcash. In: 2019 IEEE Conference on Communications and Network Security (CNS). pp. 118–123. IEEE (2019)
109. Herrera-Joancomarti, J., Navarro-Arribas, G., Ranchal-Pedrosa, A., Perez-Sola, C., Garcia-Alfaro, J.: On the difficulty of hiding the balance of lightning network channels. Cryptology ePrint Archive, Report 2019/328 (2019), https://eprint.iacr.org/2019/328
110. Moreno-Sanchez, P., Kate, A., Maffei, M., Pecina, K.: Privacy preserving payments in credit networks. In: Network and Distributed Security Symposium (2015)
111. Moreno-Sanchez, P., Zafar, M.B., Kate, A.: Listening to whispers of ripple: Linking wallets and deanonymizing transactions in the ripple network. PoPETs 2016(4), 436–453 (2016), https://doi.org/10.1515/popets-2016-0049
112. Moreno-Sanchez, P., Modi, N., Songhela, R., Kate, A., Fahmy, S.: Mind your credit: Assessing the health of the ripple credit network. In: WWW 2018. pp. 329–338 (2018)
113. Miers, I., Garman, C., Green, M., Rubin, A.D.: Zerocoin: Anonymous distributed e-cash from bitcoin. In: Symposium on Security and Privacy. pp. 397–411 (2013)
114. Wiki, B.: Bitcoin mixing (2018), available at: https://en.bitcoin.it/wiki/Mixing_service
115. Wiki, B.: Coin join (2019), available at: https://en.bitcoin.it/wiki/CoinJoin

116. Ruffing, T., Moreno-Sanchez, P., Kate, A.: Coinshuffle: Practical decentralized coin mixing for bitcoin. In: European Symposium on Research in Computer Security. pp. 345–364. Springer (2014)
117. Ruffing, T., Moreno-Sanchez, P., Kate, A.: P2P mixing and unlinkable bitcoin transactions. In: Network and Distributed System Security Symposium (2017)
118. Ruffing, T., Moreno-Sanchez, P.: Valueshuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin. In: BITCOIN Workshop. pp. 133–154 (2017)
119. Moreno-Sanchez, P., Ruffing, T., Kate, A.: Pathshuffle: Credit mixing and anonymous payments for ripple. PoPETs 2017(3), 110 (2017)
120. Ziegeldorf, J.H., Grossmann, F., Henze, M., Inden, N., Wehrle, K.: Coinparty: Secure multi-party mixing of bitcoins. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, CODASPY 2015, San Antonio, TX, USA, March 2-4, 2015. pp. 75–86 (2015), https://doi.org/10.1145/2699026.2699100
121. Danezis, G., Serjantov, A.: Statistical disclosure or intersection attacks on anonymity systems. In: International Workshop on Information Hiding (2004)
122. Zhang, Y., Long, Y., Liu, Z., Liu, Z., Gu, D.: Z-channel: Scalable and efficient scheme in zerocash. Computers & Security (2019)
123. Zcash, available at: https://z.cash/
124. Wüst, K., Gervais, A.: Ethereum eclipse attacks. Tech. rep., ETH Zurich (2016)
125. Gervais, A., Ritzdorf, H., Karame, G.O., Capkun, S.: Tampering with the delivery of blocks and transactions in bitcoin. In: Conference on Computer and Communications Security. pp. 692–705. ACM (2015)
126. Rohrer, E., Malliaris, J., Tschorsch, F.: Discharged payment channels: Quantifying the lightning network's resilience to topology-based attacks. CoRR abs/1904.10253 (2019), http://arxiv.org/abs/1904.10253
127. Kumaresan, R., Bentov, I.: Amortizing secure computation with penalties. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. p. 418429. CCS 16, Association for Computing Machinery, New York, NY, USA (2016), https://doi.org/10.1145/2976749.2978424
128. Kiayias, A., Litos, O.S.T.: A composable security treatment of the lightning network. Cryptology ePrint Archive, Report 2019/778 (2019), https://eprint.iacr.org/2019/778
129. Ben-Sasson, E., Chiesa, A., Tromer, E., Virza, M.: Succinct non-interactive zero knowledge for a von neumann architecture. In: 23rd {USENIX} Security Symposium ({USENIX} Security 14). pp. 781–796 (2014)
130. Buterin, V.: On-chain scaling to potentially 500 tx/sec through mass tx validation (2018), available at: https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477
131. ZmnSCPxj: [lightning-dev] an argument for single-asset lightning network (2018), available at: https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-December/001752.html
132. Spilman, J.: [bitcoin-development] anti dos for tx replacement (2013), available at: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-April/002433.html
133. McCorry, P., Möser, M., Shahandasti, S.F., Hao, F.: Towards bitcoin payment networks. In: Australasian Conference on Information Security and Privacy. pp. 57–76. Springer (2016)

134. Decker, C., Russell, R., Osuntokun, O.: Eltoo: A simple layer2 protocol for bitcoin (2018), available at: https://blockstream.com/eltoo.pdf
135. Bentov, I., Kumaresan, R., Miller, A.: Instantaneous decentralized poker. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 410–440. Springer, Advances in Cryptology ASIACRYPT 2017 (2017)
136. McCorry, P., Buckland, C., Bakshi, S., Wüst, K., Miller, A.: You sank my battleship! a case study to evaluate state channels as a scaling solution for cryptocurrencies (2019), available at: https://pdfs.semanticscholar.org/284e/2003a93836ae70c1af0ae922bd9d62473f75.pdf
137. Close, T., Stewart, A.: Forcemove: an n-party state channel protocol (2018)
138. Bentov, I., Kumaresan, R.: How to use bitcoin to design fair protocols. In: Annual Cryptology Conference. pp. 421–439. Springer (2014)
139. Wiki, B.: Hashed timelock contracts (2019), available at: https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts
140. Poelstra, A.: Lightning in scriptless scripts. Mailing list post, https://lists.launchpad.net/mimblewimble/msg00086.html
141. Zamyatin, A., Harz, D., Lind, J., Panayiotou, P., Gervais, A., Knottenbelt, W.: Xclaim: Trustless, interoperable, cryptocurrency-backed assets. In: IEEE Security and Privacy. IEEE (2019)
142. Moreno-Sanchez, P., RandomRun, Le, D.V., Noether, S., Goodell, B., Kate, A.: DLSAG: non-interactive refund transactions for interoperable payment channels in monero. IACR Cryptology ePrint Archive 2019, 595 (2019), https://eprint.iacr.org/2019/595
143. Goldschlag, D., Reed, M., Syverson, P.: Onion routing for anonymous and private internet connections. Communications of the ACM 42(2), 39–40 (1999)
144. Maymounkov, P., Mazieres, D.: Kademlia: A peer-to-peer information system based on the xor metric. In: International Workshop on Peer-to-Peer Systems. pp. 53–65. Springer (2002)
145. Ahuja, R.K., Magnanti, T.L., Orlin, J.B.: Network flows. Cambridge, Mass.: Alfred P. Sloan School of Management, Massachusetts (1988)
146. Tsuchiya, P.F.: The landmark hierarchy: a new hierarchy for routing in very large networks. In: SIGCOMM Computer Communication Review. vol. 18, pp. 35–42. ACM (1988)
147. Papadimitriou, C.H., Ratajczak, D.: On a conjecture related to geometric routing. Theoretical Computer Science 344(1) (2005)
148. Dong, M., Liang, Q., Li, X., Liu, J.: Celer network: Bring internet scale to every blockchain. arXiv preprint arXiv:1810.00037 (2018)
149. Wang, P., Xu, H., Jin, X., Wang, T.: Flash: Efficient dynamic routing for offchain networks. arXiv preprint arXiv:1902.05260 (2019)
150. Hoenisch, P., Weber, I.: Aodv–based routing for payment channel networks. In: International Conference on Blockchain. Springer (2018)
151. Roos, S., Beck, M., Strufe, T.: Anonymous addresses for efficient and resilient routing in f2f overlays. In: Conference on Computer Communications. pp. 1–9 (2016)
152. Werman, S., Zohar, A.: Avoiding deadlocks in payment channel networks. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology (2018)
153. Osuntokun, O.: Amp: Atomic multi-path payments over lightning, available at: https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-February/000993.html

154. Interledger, available at: https://interledger.org/
155. Piatkivskyi, D., Nowostawski, M.: Split payments in payment networks. In: Garcia-Alfaro, J., Herrera-Joancomartí, J., Livraga, G., Rios, R. (eds.) Data Privacy Management, Cryptocurrencies and Blockchain Technology. pp. 67–75. Springer International Publishing, Cham (2018)
156. Khalil, R., Gervais, A., Felley, G.: Tex–a securely scalable trustless exchange
157. Robinson, D.: Plasma debit: Arbitrary-denomination payments in plasma cash (2018), available at: https://ethresear.ch/t/plasma-debit-arbitrary-denomination-payments-in-plasma-cash/2198
158. Rao, B.: Gluon plasma: a plasma variant for non-custodial exchanges (2018), available at: https://leverj.io/GluonPlasma.pdf
159. Jones, B., Fichter, K.: More viable plasma (2018), available at: https://ethresear.ch/t/more-viable-plasma/2160
160. Plasma snapp - fully verified plasma chain (2018), available at: https://ethresear.ch/t/plasma-snapp-fully-verified-plasma-chain/3391
161. Chaum, D.: Blind signatures for untraceable payments. In: Advances in cryptology. pp. 199–203. Springer (1983)
162. Chaum, D., Fiat, A., Naor, M.: Untraceable electronic cash. In: Conference on the Theory and Application of Cryptography. pp. 319–327. Springer (1988)
163. Yang, B., Garcia-Molina, H.: Ppay: micropayments for peer-to-peer systems. In: Proceedings of the 10th ACM conference on Computer and communications security. pp. 300–310. ACM (2003)
164. Browne, R.: Big transaction fees are a problem for bitcoin but there could be a solution (2017), available at: https://www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html
165. Fromknecht, C.: 2p-ecdsa: Two-party ecdsa multisignatures. Github project, https://github.com/cfromknecht/tpec
166. Gervais, A., Karame, G.O., Capkun, V., Capkun, S.: Is bitcoin a decentralized currency? IEEE security & privacy 12(3), 54–60 (2014)
167. Gencer, A.E., Basu, S., Eyal, I., Van Renesse, R., Sirer, E.G.: Decentralization in bitcoin and ethereum networks. arXiv preprint arXiv:1801.03998 (2018)
168. Roll-up, available at: https://github.com/barryWhiteHat/roll_up

Appendix A Channels

A.1 Payment Channels

Here we present in detail the evolution of payment channel designs.

Replace by Incentive Spilman [132] presented the first major step towards secure (unidirectional) payment channels based on the ***RbI*** mechanism, implemented in Bitcoinj [22, 23]. This channel allows a sender to issue payments to a recipient, but the recipient cannot send the funds back through the same channel. To create a channel, the sender locks a deposit on-chain. The deposit can be refunded (i.e. the channel closed) if one of the following two conditions are met: *(i)* the sender retrieves their deposit after time t or *(ii)* both the sender and receiver authorize the release of the deposit. The channel state is represented as the balance of funds of both parties within the channel. To issue a payment,

the sender signs a new state that monotonically decrements the sender's balance and monotonically increments the receiver's balance. The signature and the new state are sent to the receiver who can either *(i)* immediately sign and publish on-chain the new state to claim the payment, or *(ii)* wait for a new state from the sender that pays more coins. For the recipient, it is safe to wait for new states from the sender, because the on-chain deposit cannot be refunded to the sender until time t is reached[15]. The sender can continuously send new payments to the receiver until either the sender's balance is depleted or the receiver decides to close the channel before time t. When closing the channel, a rational receiver publishes the latest received state to settle with the highest amount of coins. To our knowledge, unidirectional payment channels are the only type of channel that allow the sender to remain safely offline, without the risk of losing funds. The throughput (number of transactions) of a unidirectional payment channel is limited by the size of the sender's deposit and the smallest denomination of the cryptocurrency asset. A deposit of e.g. 1 coin allows at most 10^8 transfers assuming a minimum denomination of 10^{-8}.

A *pair* of ***RbI*** channels can be combined to support bidirectional payments [27]. Unlike single ***RbI*** channels, the sender increments coins owed to the receiver and the value can go beyond the sender's deposit. When the channel is closed, the smart contract computes the offset of the coins owed in both ***RbI*** channels before sending each party their final balance.

Replace by Time Lock In a UTXO-based blockchain, ***RbT*** allows the construction of bidirectional payment channels. Each state update is associated with a time lock, which prevents the transaction's acceptance into the blockchain, until some predefined time in the future. When the payment direction within the channel changes, the time lock associated to the new state update is decremented by an amount Δ, the *safety time gap* (cf. Figure 4). While ***RbT*** enables rapid micro-payments, this mechanism suffers from notable limitations. The party receiving the final state update must be online at precisely time t to claim and publish the latest payment on the blockchain. If the latest state does not get accepted within Δ time (i.e. due to blockchain congestion), the counterparty has an opportunity to broadcast an older state update, attempting to reverse the final payment. The choice of Δ and the number of payment direction changes limit the channel's transaction throughput ceiling.

To alleviate these concerns, Decker and Wattenhofer [24] propose *Invalidation Trees* combining ***RbI*** and ***RbT***, known as Duplex Micropayment Channels (DMC). Bidirectional payments (or duplex payments) are processed via a pair of ***RbI*** payment channels. When one channel exhausts its supply of coins, the channels can be *reset* by destroying the current state and re-creating a suitable state update for the pair of one-way payment channels in an off-chain manner via an invalidation tree. Each node in the tree has a time lock, and the branch with the lowest time lock is first accepted into the blockchain before the other branches. An alternative version of DMC [37] proposes to remove the channel's

[15] Note that the blockchain acts as coarse time-stamping service.

fixed expiry time and support n parties. There exists an inherent trade-off between the number of channel resets and the branch nodes required to broadcast in the event of a dispute. The worst-case dispute requires the entire branch to be published with $n + 2$ states, given n nodes in the invalidation tree and two *RbI* channels. Parties must be online during the safety time gap to ensure the latest branch is written to the blockchain.

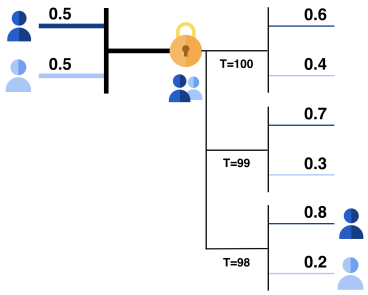

Fig. 4. Time lock-based payment channels in an UTXO model. Lowest time lock transactions are included on-chain first.

Replace by Revocation Poon and Dryja propose Lightning channels to overcome the previous state replacement channel throughput limitations and to remove expiry times [25, 133] (cf. Figure 5). We refer to Lightning channels as *RbR*, because both parties agree on the channel's new state before revoking the old state. To revoke, both parties exchange revocation secrets (i.e. a preimage of a hash) and retain those during the channel's lifetime. A penalty mechanism discourages parties from broadcasting older states. If one party broadcasts a revoked state, the blockchain accepts within a time-window proofs of maleficence from the other party. A successful dispute grants the winning party *all* coins of the channel. *RbR* is the first channel design to require both parties to remain online and fully synchronized with the blockchain to observe malicious closure attempts. Unfortunately, *RbR* introduces unfavorable implications for third-party watching services (cf. Section 8). With N being the number of channel updates, *RbR* entails $O(N)$ storage as the watching service must store evidence for every in-channel update to prove an authorized state as revoked.

Replace by Version (UTXO-blockchains) Decker *et al.* propose Eltoo [134] to support *RbV* for UTXO-based blockchains through the use of *floating transactions*, i.e. transactions attachable to an output of any preceding transaction. With the possibility of linking established updates, the Eltoo technique utilizes *state numbers* to impose time ordering on the updates and supports the storing of temporary state. As with Lightning channels, there is no expiry time and no limitation on the channel's throughput. Its closure dispute process is similar to that of state channels (cf. next Section) and there is no penalty for publishing replaced states. Watching services can verify a newly received state with $O(1)$ storage costs, requiring only the state with the largest state number.

A.2 State Channels

State channels extend the payment channel concept towards the execution of *arbitrary* applications (e.g. [135]) and typically involve two smart contracts: one

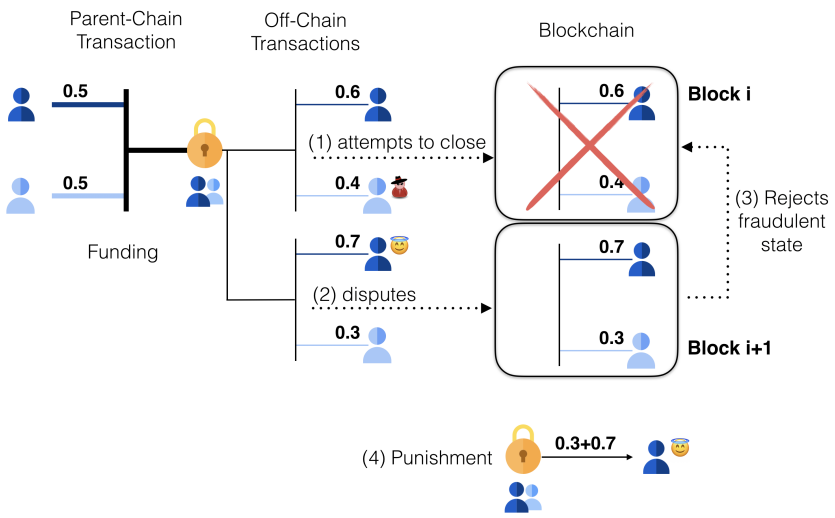

Fig. 5. Payment channel construction based on a punishment scheme [25]. If a malicious channel party (1) attempts to close the channel with an outdated state, the other channel party can (2) dispute the closure, and (3) reject the fraudulent closure. The honest party (4) receives the total channel balance.

for the state channel itself and one for the to be executed application. Known state channels rely upon *RbV* as the state replacement technique and thus entail $O(1)$ storage requirements for watching services. To the best of our knowledge, only Sprites [28] and Perun [29, 82] offer formal security proofs. We distinguish between *closure disputes* and *command disputes*.

Closure Disputes In a *closure dispute*, one party triggers a dispute to close the channel and to continue the application's execution exclusively on layer-one. Perun proposes two-party state channels that support installing/uninstalling application smart contracts off-chain [29]. Its dispute process focuses on a single application and enforces a fixed time window for involved parties to submit collectively authorized states for the application with the largest version (i.e. *RbV*). After the time window, any party can resolve the dispute. This re-deploys and continues the application's smart contract with its current state on the blockchain [29]. To install an application, both parties collectively sign the application's new state, the number of coins allocated to it, and its initial version. To uninstall the application, both parties authorize a state that terminates it and de-allocates the coins. The coins are only unlocked based on the outcome of the conditional application smart contract. Kitsune [136] relies on the same closure dispute process but is designed to support n parties and relies on an existing smart contract on the blockchain.

Command Disputes A command dispute aims to execute a specific command on the parent-chain, and then resume execution off-chain. The channel thus does not close and can continue its off-chain execution after the command executes [28]. The blockchain grants a pre-determined time window to collect commands from each party and all commands execute after the dispute process expires. After the dispute, the state version increments, and the new state transition is considered the newest channel state. Note that a state with a newer *RbV* version can cancel the dispute process.

PISA [68] reduces Sprite's [28] dispute costs by allowing parties to submit a hash of the state. Arbitrum [44] removes the overhead for an honest party to send the full state to the blockchain, instead the honest party can assert the hash of a new state alongside the command and its input. Counterfactual's [76] (and others [137]) command dispute process allows the execution of multiple commands by extending the dispute process expiry time depending on the number of commands [76]. While Counterfactual allows parties to install and uninstall multiple applications off the chain, it is restricted to two parties and turn-based applications.

Appendix B Channel synchronization

Hashed Time-Locked Contracts (HTLCs). HTLC [24, 138, 139] enable cross-channel synchronization by allowing A to lock x coins from A and B's channel that are only redeemable if the contract's conditions are fulfilled. The conditions of the contract $HTLC(A, B, y, x, t)$ rely on a collision-resistant hash function H, a hash value $y = H(S)$, where S is chosen uniformly at random, the amount of coins x and a timeout t. If B produces a value S such that $H(S) = y$ before timeout t expires, B gets the locked x coins. Otherwise, if timeout t expires, the locked x coins go back to A. Let's assume that A wants to send a payment to C using B as intermediary and there exist channels between A, B and B, C. The receiver C generates a secret S and provides the initial sender, A, with the hash of the secret $H(S)$. A can then establish a HTLC with B, the next hop, which B may spend under the condition that he can provide A with the preimage of $H(S)$ before a set expiry date, generally expressed in number of blocks. Should B fail to provide the requested input in time, A is able to commit a refund transaction on-chain. B then constructs a similar HTLC with C with two main differences: *(i)* the lock period of the HTLC output is reduced, thereby ensuring that B has enough time to claim the funds from the previous hop; and *(ii)* the amount of coins locked in this HTLC is reduced. The difference in locked coins corresponds to the service fee charged by B for the forwarding of the payment. As C is the final receiver, C can safely reveal S to B, who then has a sufficient period of time to reveal a pre-image. HTLCs can be used for paths of an arbitrary number of channels and are integrated in Lightning [25] and DMCs [24].

A key concern for HTLCs is whether sufficient collateral is available when setting up a path. Every hop along the path includes *an additional* time-delay to ensure the hop can always retrieve their coins from the previous hop after

sending their coins to the next hop. The longer the payment path, the more collateral must be reserved. In the worst-case, the collateral cost is $\theta(l^2 X\Delta)$, where l is the number of channels, X is the payment amount and Δ is the time that an on-chain transaction takes longer than an off-chain exchange.

Global Preimage Manager. Miller et al. [28] introduce a *PreimageManager* smart contract that allows a single dispute to atomically finalize the synchronized transfer for all hops along the path. This reduces the collateral lock up time for synchronizing a payment across l channels to $\theta(lX\Delta)$. The smart contract accepts the preimage of a hash and stores it alongside a timestamp. All parties along the path introduce a new conditional transfer that asserts the transfer is only considered complete if *the preimage x of hash $h = H(x)$ was published in the PreimageManager before time t*. A single dispute at any position along the path can use the published value x before time t to reach an agreement about the new state. In contrast to HTLCs, all channels along the payment route can re-use the same condition for their transfer without waiting for each other. Sprites converts disputes as local events in each channel to a single global event, guaranteeing that all channels share the same worst-case expiry time.

Scriptless Multi-Hop Locks. HTLC-based synchronization protocols are limited to connect channel constructions with the same hash function (e.g. SHA256). HTLCs also suffer from the severe wormhole attack, which prevents users from successfully executing the synchronization protocol and allows an adversary to steal the synchronization reward [79].

A Multi-Hop Lock (MHL) [79] is an alternative synchronization mechanism that enables cross-channel synchronization. Like a HTLC, a MHL allows A to lock x coins in A and B's channel that can only be released if a set of conditions are fulfilled. The crux of MHL is that the cryptographic hardness condition is no longer encoded in the underlying blockchain's scripting language (and thus it is called *scriptless* in the blockchain folklore). The scriptless locks stem from Poelstra [140] who provided a way to embed certain contracts into Schnorr signatures. Malavolta et al. [79] formalized this construction, proposed alternative constructions relying on ECDSA signatures and one-way homomorphic functions and enabled the combination of locks with different signatures in one payment path. This approach enables interoperable [141] locks across all blockchains that support a digital signature scheme such as ECDSA or Schnorr to authorize transactions. Moreover, this approach provides provable security, privacy guarantees and solves the wormhole attack (cf. Section 8). The conditions of *MHL(A, B, x, m, pk, t)* depend on a message m, a public key pk of a given signature scheme and a timeout t. If B produces a valid signature σ of m under pk before timeout t expires, B receives the locked x coins. Otherwise, if timeout t expires, the locked x coins are returned to A. Recent work [142] shows how to build the MHL contract leveraging linkable ring signatures, the digital signature scheme used in the Monero cryptocurrency.

Appendix C Routing Algorithms

In the following, we describe each algorithm in detail and focus on the aspects of effectiveness, efficiency, and scalability. As outlined in Appendix G Table A2, only one algorithm class explicitly considers cost-effectiveness. While others like SpeedyMurmurs [31] implicitly achieve low fees by selecting short paths if fees are homogeneous, the algorithm design and evaluation do not include this aspect. Similarly, only SilentWhispers [30] and SpeedyMurmurs [31] introduce concrete notions of privacy (cf. Section 7). Some algorithms involve the use of onion routing [27, 32, 34], which requires the random selection of nodes in a path to achieve its anonymity guarantees [143]. As routing algorithms do not select nodes randomly, it remains unclear if onion routing provides privacy in the context of payment channels (cf. Section 7 for our privacy observations).

Global View. Lightning [25] and Raiden [27] use *Source Routing* [33], in which the source of a payment specifies the complete route for the payment. If the global view of all nodes is accurate, source routing is highly effective because it finds all paths between pairs of nodes. However, by default source routing does not consider channel balances, and routing decisions might contain channels with low balances or implicitly turn bidirectional channels into unidirectional ones, reducing the available routes over time in a dynamic PCN.

SpiderNetwork [32] improves the effectiveness of source routing in a dynamic PCN by introducing three key modifications: i) the choice of the routes includes a bias towards routes that optimize the balance, ii) routing includes on-chain rebalancing, meaning that nodes deposit additional coins to improve the balance, and iii) routing relies on a packet-switched network, i.e. instead of routing a complete payment, the algorithm splits the payment into constant-size units and routes each of them individually. SpiderNetwork is therefore highly effective even when balances are constantly changing, at the cost of higher latencies if on-chain rebalancing is used.

Similarly, Di Stasi et al. [86] model multi-path source routing as an optimization problem but focus on minimizing fees. Furthermore, they define fee policies that improve the balance. Their simulations based on a network of only 200 nodes indicate that their algorithm provides lower fees and a better balance than Lightning's source routing. However, the authors do not consider any metrics apart from fees and balance. We do not include the paper in Appendix G Table A2 as i) the evaluation lacks the necessary information and ii) being a source routing algorithm, the approach shares the properties of Lightning's algorithm but achieves higher effectiveness. By pre-computing paths locally, algorithms based on a global view exhibit low latencies and communication overheads. However, the local memory costs of storing the ever-complete snapshot and computation costs for finding paths (and solving an optimization problem cf. SpiderNetwork) are high. The same holds for the overhead resulting from opening or closing a channel on-chain, and these overheads increase super-linearly in the number of nodes and limit scalability.

Local View. Algorithms based on local information use well studied concepts: *(i)* distributed hash tables (DHTs) [144], *(ii)* flow algorithms [145], *(iii)* (ad-hoc on-demand) distance vector routing, *(iv)* landmark routing [146] and *(v)* network embeddings [147].

Flare [35] leverages the Kademlia DHT [144]. Kademlia in its original form opens new channels between strategically chosen nodes, which is expensive in terms of latency and on-chain fees. Flare, therefore, uses a modified Kademlia version that replaces direct channels with multi-hop paths, which does not require opening new channels. This modification results in longer routes, higher latencies and communication overheads compared to traditional DHTs. The likely most significant limitation of Flare is its inability to support topology changes. We did not include Flare in Appendix G Table A2 as the algorithm lacks the ability to consider dynamics adequately and hence does not constitute a full solution.

There are two algorithms based on flow algorithms: Celer [148] and Flash [149]. Flash differentiates payments based on the payment value. If a payment has a high transaction value, Flash uses a modification of the EdmondsKarp algorithm for computing an approximation of the maximal flow that finds at most k paths for a constant k. The modification decreases the communication complexity from $|V||E|$ to $k|E|$ for a channel network of $|V|$ nodes and $|E|$ channels. As the algorithm executes k distributed breath-first searches, it has a high latency. Otherwise, if a payment has a low transaction value, Flash routes the payment based on local routing table and hence avoids an expensive flow algorithm. Nevertheless, assuming that the fraction of payments with large transaction values is constant, the algorithm scales linearly in the number of channels rather than logarithmically like other algorithms.

Celer's routing relies on a flow algorithm, *cRoute*. An optimization problem is formulated based on local congestion with solutions guided by the congestion gradients. The algorithm is effective and keeps channels balanced. As the evaluation of cRoute only considers 77 nodes [148], we cannot make conclusive statements about its scalability, related work indicates problems with efficiency and scalability [31, 145].

In a distance vector routing protocol, each node maintains a routing table to all other nodes, meaning that any update requires changes to all routing tables. Ad-hoc on-demand distance vector (AODV) routing reduces this cost by only filling routing tables when searching for a route. Hoenisch and Weber [150] explore ad-hoc on-demand distance vector routing for payment networks but limit their evaluation to the random graphs of maximally 5,000 nodes. The results indicate a high effectiveness both in regard to successful path discovery and cost. However, even for those comparable small graphs, the communication overhead is high, so that scalability is unlikely. We did not include AODV in the table as there is no evaluation in comparison to alternative algorithms available and it is hence unclear how to judge the reported performance.

SilentWhispers [30] implements landmark routing, where landmarks are dedicated nodes. Each node keeps track of the neighbor to contact to reach all land-

marks. A payment between two nodes first traverses the path from the sender to the landmark and then from the landmark to the receiver. Using multiple landmarks in combination with multi-party computation enables payments to be split over multiple paths in a privacy-preserving manner. Each node periodically recomputes how to reach the landmarks to account for topology changes. However, as recomputation is not necessary for every topology change, the costs of updates are lower than source routing. The evaluation of SilentWhispers on a real-world dataset reveals low effectiveness and moderate latencies in comparison to other algorithms [31]. Multi-party computation, required for each transaction, involves computation costs and results in low scalability when increasing the number of transactions.

Aiming to overcome the drawbacks of SilentWhispers, SpeedyMurmurs [31] uses embedding-based routing and a protocol for handling topology updates locally. Nodes express their position in a rooted spanning tree through coordinates and locally choose the next node in a payment path by considering all adjacent channels with sufficient balance. Among these channels, nodes then select the channel to the node with the coordinate closest to the recipient's coordinate. While the coordinate assignment results from the underlying spanning tree, the path can contain channels that are not part of the spanning tree. In this manner, SpeedyMurmurs exhibits high effectiveness and low latencies for a static PCN. As SpeedyMurmurs blocks funds while conducting payments, high transaction frequencies might be affected due to locked funds. If a channel opens or closes, only descendants in the underlying spanning tree have to adjust their coordinates, which typically results in an overhead that is logarithmic in the network size [151]. However, SpeedyMurmurs does not consider balances, which results in low effectiveness due to insufficient balances in a dynamic PCN [32, 148].

Deadlocks. Deadlocks may arise on concurrent payments that proactively block deposits on channels [152]. For instance, assume that A and B conduct concurrent payments and both choose paths that contain the channels c_1 and c_2. Furthermore, c_1 and c_2 have sufficient collateral to complete either but not both payments. Now, if A's payment blocks funds of c_1 before B's payment does and B's blocks funds of c_2 first, both payments fail. In the context of source routing, a suggested solution [152] is to design a global partial order $<$ on the set of channels, while it is unclear how to adapt the proposal to routing protocols relying on a local view.

Multi-path Routing. Networks typically spawn multiple paths from a node A to a node B that routing may find. Existing algorithms fall under the following categories: *(i)* single-path routing algorithm [25] where the success of a payment is subject to the credit available on a single path, *(ii)* multi-path routing that explicitly split the payment amount into multiple smaller concurrent transfers [30, 31, 153]) thereby reducing the capacity required on each path; and *(iii)* packet-switched routing that routes each unit of payment individually and

incrementally transfers the funds (i.e., an approach known as *streaming micropayments*) [32, 154][16].

A partial evaluation indicates that packet-switched networks provide the best performance with regard to effectiveness [155]. The evaluation is limited to source routing and does not evaluate packet-switching for alternative routing algorithms. These results indicate that packet-switched routing algorithms is a promising direction of future research.

To our knowledge, no routing algorithm fulfills all desired criteria. Algorithms requiring a global view have inherent scalability issues. Algorithms based on a local view are scalable but are bound to provide lower effectiveness and efficiency. While the existing algorithms exhibit low performance or lack in-depth evaluations, they represent the first application of key routing concepts to payment and state channels. In particular, there is no inherent reason why coordinate-based routing algorithms cannot achieve high effectiveness in dynamic PCN settings. Future research accounting for channel balances may have the potential to overcome such issues. Rebalancing algorithms that transfer funds along circular paths are also an approach worth further investigation [36].

Appendix D Commit-chains

D.1 NOCUST

NOCUST [26] is an account-based commit-chain where an on-chain address is associated to a commit-chain account. The NOCUST on-chain contract expects to periodically receive a constant-sized commitment to the state of the commit-chain ledger from the operator, containing each user's account in the collateral pool. The commitment to this (potentially) large state is constructed such that it is efficient to prove and verify in the smart contract that a user's commit-chain account was updated correctly by the operator, such that transfers, withdrawals and deposits can be securely enacted. Users can deposit any amount of coins within the contract, and perform commit-chain payments of any denomination towards other users. TEX extends NOCUST to support atomic commit-chain swaps [156].

Efficient *lightweight clients* in NOCUST only need to verify their respective account balance. NOCUST proposes *free establishment*, wherein a user can join the commit-chain without on-chain transaction and immediately receive commit-chain transactions. Regarding *agreed transition*, a transaction within NOCUST is enacted with the signature of the sender and the operator to deter potential double-spend scenarios. NOCUST provides *balance security* towards honest users, even if the operator and all other commit-chain users collude. A transaction is considered final when the sender and operator agree to the payment, and the payment is committed within the periodic on-chain checkpoint. NOCUST

[16] Interledger [154] is not strictly a layer-two protocol, since as a protocol it is not necessarily tethered to a layer-one blockchain, instead seeking to operate on top of 'ledgers' construed more broadly, to include traditional custodial bank ledgers.

only offers *state progression* if the operator stakes collateral towards the recipient. To this end, NOCUST specifies a mechanism to allocate collateral towards all commit-chain users within a constant-sized on-chain commitment, enabling instant transaction finality for the specified amounts. The allocated collateral is *re-usable* after each checkpoint. The transaction throughput is only limited by the operator's bandwidth and computational throughput, and independent of the checkpoint commitment interval. While NOCUST users are not required to be constantly online, they are expected to monitor the blockchain at regular time intervals to observe the checkpoint commitments for *commitment integrity*. Each user is only required to verify their respective balance proof by requesting data directly from the operator and comparing it to the locally stored state. In the case of any misbehavior, a user can always issue a challenge using the NOCUST smart contract to force the operator to promptly answer this challenge with valid information. If the operator responds to the challenge with invalid information (or does not respond), users have an accountable and public proof of misbehavior on-chain. To strengthen the operator's integrity, NOCUST supports a provably consistent mode of operation through the use of zkSNARKS. As such, the underlying smart contract validates layer-two state transitions and the operator is not able to commit to invalid state transitions, without being halted by the smart contract.

D.2 Plasma

Plasma [38] is a high-level specification of a UTXO-based commit-chain. Following the initial proposal, a variety of alternatives are informally discussed [67, 157–160]. We only discuss Plasma Cash [87] as it is the most comprehensive working draft. In this system, all coins are represented as serial numbers and every transfer allocates a new owner for the respective coin. A coin is minted with an on-chain deposit and cannot be merged or splitted with another coin on the commit-chain. This limitation reduces the practical applicability as a payment system (but is helpful for non-fungible tokens) and several coins may be required to facilitate a single transfer. Plasma Cash therefore resembles classical e-cash protocols [161–163] with fixed coin denomination.

In terms of *agreed transition*, a transfer is incomplete until the recipient has verified the *entire* coin transaction history (which needs to be transmitted off-chain), the transaction is included in a hash commitment in the parent-chain and the hash commitment's pre-image is shared with the user. Plasma Cash supports *free establishment* as coins can simply be assigned a new owner. While there is no mechanism to challenge the integrity of a hash commitment by the operator to achieve *commitment integrity*, all users can detect invalid commitments and it is expected that they eventually withdraw their coins from the commit-chain. If an operator commits to an invalid coin transfer and tries to withdraw it, the coin's owner can also issue a withdrawal for the same serial number based on a previous hash commitment. If the operator cannot prove to the parent-chain that the coin was spent, then their invalid transfer withdrawal is cancelled, and the rightful owner receives the coins. In addition, if a party tries to withdraw an already

spent coin, then the coin's current owner can prove to the blockchain that it was already spent. Thus, it appears that Plasma Cash achieves *balance security* as an honest party can always withdraw their coins from the commit-chain, even if an invalid commitment is posted. In addition, the owner must keep the entire transaction history for each coin and confirm all transactions are confirmed in the commit-chain. Finally, each commitment can only include a single transfer per coin as the operator is not trusted to prevent double-spends and thus the transaction throughput relies on the on-chain commitment frequency. A Plasma Cash transaction can be sent to any (parent-chain) address, without particular registration requirements. If the recipient has not yet installed a compatible plasma wallet, the sender is assumed to notify the recipient to watch out for their commit-chain funds. Note that a transfer is not considered confirmed or secure until the recipient has verified the coin's entire transaction history within the commit-chain. Plasma Cash does not specify a method to provide *state progression*.

Appendix E Security Threats

Hot Wallets. Channels require unanimous agreement for state updates and thus need all involved parties to be online with access to their signing keys. Keeping keys online in a *hot wallet*, i.e. a list of private signing keys, is critical — parties become prime targets for adversaries. This may potentially limit the capacity of PCN as channel operators must exercise caution about the number of coins they are willing to risk. While parties in commit-chains face similar challenges, the commit-chain operator is not required to stake assets to facilitate payments (when providing delayed transaction finality) — and receivers in e.g. NOCUST can moreover remain offline at the time of payment.

Online Assumption. One concern for layer-two protocols is the assumption that parties remain online and fully synchronized with the PCN and blockchain. With the exception of ***RbI*** and ***RbT***, channel designs require parties to watch for malice closures with outdated states. For commit-chains, users are required to either surface online in periodic intervals (i.e. each *eon* in NOCUST) or to watch the blockchain continuously for malicious exits [67]. If parties fail to monitor the layer-two protocol, the commit-chain operator can perform *execution forks* [68] to steal the offline user's assets. Watching services alleviate the online assumption (cf. Section 3.3).

Blockchain Reliability and Mass Exits. Layer-two designs assume that the underlying blockchain accepts transactions eventually. Miners include transactions based on fees and under network congestion, transaction fees can grow from several cents to $50 [164]. Under congestion, parties may fail to meet deadlines to settle disputes and for PCN/PCH this might result in unfairly closed channel states. Under a mass exit (e.g. when many users close channels), blockchain users might enter in a bidding-war for their on-chain exit transactions to confirm.

Commit-chain operators are single points of availability failure and require, if halted, all users to withdraw their assets. Contrary to PCN, commit-chains do not require a deadline for users to withdraw their coins, mitigating the transaction fee bidding war. A NOCUST operator is forced by the smart contract to halt given one successful dispute by a user, allowing all users to exit fairly. A Plasma Cash operator is not halted, even if operator's misbehavior is provably reported.

Security of Synchronizing Protocols. One concern with HTLCs-based protocols is the *wormhole attack* [79] that allows an adversary situated in a multi-hop payment path to steal transaction fees by excluding the honest users from the successful completion of a payment. The adversary thereby forces the honest user to lock coins during the payment commit and bypasses the user during the release phase of a payment. The Lightning Network is currently vulnerable and the AMHL protocol is being considered to mitigate this issue [165]. Recent work [80] shows how to achieve the atomicity property for a PCH [81] and for Bitcoin-compatible PCNs while reducing the collateral required in multi-hop payments.

Another concern with synchronizing payments, *the American Call Option attack*, is that an adversary can set up a multi-hop payment and not release the trigger to finalize the payment. As a result, the coins are locked up until the transfer's expiry time and the adversary can perform this lock-up for free as all coins are refunded. Thus there is a loss of opportunity cost as the coins are locked up.

Appendix F Open Challenges

In light of our holistic overview of the current layer-two literature, we identify the following avenues of future research as open challenges.

Layer-Two Cost Quantification: A comprehensive study of the real economic costs of layer-two transactions, ideally comparing different channel, synchronization and commit-chain proposals. Only if the layer-two transaction fees and security concerns are inferior to the offered on-chain, then it is rational to perform layer-two transactions.

Layer-One Congestion: Existing work mostly ignores the threat of blockchain congestion. One future avenue would be to design congestion-aware [136] layer-two protocols.

Cross Commit-Chain Payments and Routing: We are not aware of work covering atomic payments across a more decentralized network of commit-chains.

Private Commit-Chain: Contrary to selected payment channel hubs [39, 41], existing commit-chains do not provide any privacy guarantees from the commit-chain operator.

Quantification of Layer-Two Decentralization: While related work discusses layer-one decentralization [166, 167], no work has yet covered layer-two decentralization.

Channel Factories on Commit-Chains: Commit-chains might enable to spawn payment channels among their users (similar to the idea of virtual channels) potentially foregoing costly channel initialization costs.

Compression-Chains: Compression-chain techniques such as Roll-up [168] aim to reduce on-chain transaction footprint. A transaction only requires 9 bytes on-chain, while a ZKP certifies the validity of signatures. While they might not be considered layer-two protocols and may not scale to the same extent, they solve data-availability concerns and strengthen the security properties. A thorough analysis of compression-chains is missing.

Formal Security/Privacy: A systematic method to develop security and privacy notions for layer-two protocols, faithfully including their interaction with layer-one, constitutes an interesting direction for future research.

Transaction Fees: There is no existing study on how rational intermediaries in channel networks would choose transaction fees and how these off-chain transaction fees interplay with on-chain fees.

Routing Algorithm Design: At the moment, no routing algorithm fulfills all requirements of interest. Future research may either develop such an algorithm or show the impossibility of achieving all requirements concurrently.

Appendix G Tables

Table A1. Overview of different channel design proposals.

	Channel technique	Throughput bottleneck	Dispute mechanism	Watchtower storage	Security proofs
RbI					
Spilman [22, 132]	Payment	Sender deposit	Closure	$O(1)$	×
Raiden [27]	Payment	Network	Closure	$O(1)$	×
RbI & RbT					
DMC [24]	Payment	Channel resets	Closure	$O(1)$	×
RbR					
Lightning [25]	Payment	Network	Closure	$O(N)$	×
RbV					
Eltoo [134]	Payment	Network	Closure	O(1)	✓
Sprites [28]	State	Network	Command	O(1)	✓
PISA Sprites [68]	State	Network	Command	$O(1)$	×
Perun [29]	State	Network	Closure	$O(1)$	✓
Counterfactual [76]	State	Network	Command	$O(1)$	×
Kitsune [136]	State	Network	Closure	$O(1)$	×

Table A2. Routing Algorithms for Multi-Hop Payments.

		Global View		Local View			
		Lightning [25]/Raiden [27]	SpiderNetwork [32]	Flash [149]	cRoute [148]	SilentWhispers [30]	SpeedyMurmurs [31]
Effectiveness	Snapshot	High	High	High	High	Medium	High
	Dynamic	Medium	High	High	High	Low	Low
Efficiency	Latency	Low	Low/High[1]	Low/High[2]	High	High	Low
	Communication	Low	Low/High[1]	Low/High[2]	High	High	Low
	Computation	High	High	Low	Low	High	Low
	Update	High	High	Low	Low	High	Low
Scalability	Nodes	Low	Low	Low	?[4]	High	High
	Transactions	High	High	Low	High	Low	Low
Cost-Effectiveness	Considered	✓	×	✓	×	×	×
Privacy	Guarantees	×	×	×	×	✓	✓

[1] High for on-chain re-balancing, otherwise low. [2] High for high-value transactions, otherwise low. [3] No evaluation, only tested for 77 nodes.

Table A3. Commit-chain properties and operational costs. Plasma data from discussions with Konstantopoulos [87].

General properties	Plasma Cash [87]	NOCUST [26]
Security proofs	✕	✓
Offline transaction reception	✓	✓
Fungible payments	✕	✓
Clients can remain offline	✕	✕(online each eon)
Instant transaction finality	✕	✓(with collateral)
Token support	✓	✓
Non-Fungible tokens	✓	✕
Provably Consistent State (ZKP)	✕	✓
Commit-Chain Swaps	✕	✓ [156]
Costs		
Parent-chain commit	Low	Low
Deposit (parent → commit-chain)	Low	Low
Withdraw (commit → parent-chain)	Low	Low
Dispute initiation	Low	Low
Dispute answer	Low	Low
User storage	High	Low
User verification	High	Low
User bandwidth	Low	Low