AN EVALUATION OF CRYPTOCURRENCY PAYMENT CHANNEL NETWORKS AND THEIR PRIVACY IMPLICATIONS

Enes Erdin[1], Suat Mercan[2], Kemal Akkaya[2]
[1]Department of Computer Science, University of Central Arkansas, Conway, AR 72035, [2]Department of Electrical and Computer Engineering Florida International University Miami, FL 33174,

NOTE: Corresponding author: Enes Erdin (eerdin@uca.edu)

Abstract *– Cryptocurrencies redefined how money can be stored and transferred among users. However, public blockchain-based cryptocurrencies suffer from high transaction waiting times and fees. To address these challenges, the payment channel network concept is touted as the most viable solution to be used for micro-payments. The idea is exchanging the ownership of money by keeping the state of the accounts locally which provides transaction approvals in seconds. Such attention on payment channel networks has inspired many recent studies that focus on how to design them and allocate channels such that the transactions will be secure and efficient. However, as payment channel networks are emerging and reaching a large number of users, privacy issues are becoming more relevant, this raises concerns about exposing not only individual habits but also businesses' revenues. In this paper, we first propose a categorization of the existing payment networks formed on top of blockchain-backed cryptocurrencies. After discussing several emerging attacks on user/business privacy in these payment channel networks, we qualitatively evaluate them based on a number of privacy metrics that relate to our case. Based on the discussions on the strengths and weaknesses of the approaches, we offer possible directions for research for the future of privacy based payment channel networks.*

Keywords – Bitcoin, blockchain, lightning network, payment channel network, routing protocols

1. INTRODUCTION

There are many modern money exchange systems such as paper checks, credit/debit cards, Automated Clearing House (ACH) payments, bank transfers, or digital cash which are owned and regulated by financial institutions. Nevertheless, in the evolving world of trade, the movement of money is still going through changes. The last decade witnessed the introduction of *Bitcoin* [1], a new paradigm-shifting innovation where the users control their own money without needing a trusted third party. In this model, the users are governing the system by coming to a consensus for controlling the transfer and the ownership of the money. Following the success of Bitcoin, new cryptocurrencies that offer new capabilities were introduced based on the idea of consensus-based account management [2, 3].

Not so long after, the initial success of cryptocurrencies was hindered due to practicality issues in their daily use. Basically, it was a very limited system in terms of scalability and its wide acceptance for simple daily transactions was quite impossible due to high confirmation waiting times, highly disproportional transaction fees, and low throughput.

Among many solutions an *off-chain payment channel* idea arose as a well-accepted one for solving the above-mentioned problems. The idea is based on establishing off-chain links between parties so that many of the transactions would not be written to the blockchain each time. The payment channel idea later evolved towards the establishment of *payment channel networks* (PCN), where among many participants and channels the participants pay through others by using them as relays, essentially forming a connected network. This is in essence a *Layer-2* network application running on top of a cryptocurrency which covers the *Layer-1* services. A perfect example of PCNs is Lightning Network (LN) [4] which uses Bitcoin and reached many users in a very short amount of time. Raiden [5], based on Ethereum, is another example of a successful PCN.

The emergence of PCNs led to several research challenges. In particular, the security of the off-chain payments is very important as users can lose money or liability can be denied. Besides, the efficiency of payment routing within the PCN with a large number of users is tackled. Such efforts paved the way for introducing many new PCNs in addition to LN. These PCNs rely on various cryptocurrencies and carry several new features. As these newly proposed PCNs become more prominent there will be heavy user and business involvement which will raise issues regarding their privacy just as the user privacy on the Internet. The difference is that in many cases, Internet privacy could be regulated but this will not be the case for PCNs as their very idea is based on decentralization. For instance, a user will naturally want to stay anonymous to the rest of the network while a business would like to keep its revenue private against its competitors.

Therefore, in this paper, we investigate this very emerging issue and provide an analysis of current PCNs along with their privacy implications. We first categorize the

PCNs in light of common network architectures and blockchain types. We then define user and business privacy within the context of PCNs and discuss possible attacks on the privacy of the participants. Specifically, we came up with novel privacy risks specific to PCNs. Utilizing these attack scenarios, we later survey and evaluate thoroughly the existing PCNs in terms of their privacy capabilities based on certain metrics. This is a novel qualitative evaluation to be able to compare what each PCN is offering in terms of its privacy features. Finally, we offer potential future research issues that can be further investigated in the context of PCN privacy. Our work not only is the first to increase awareness regarding privacy issues in the emerging realm of PCNs but also will help practitioners on selecting the best PCN for their needs.

The paper is organized as follows: Section 2 gives an introductory background. Next, Section 3 categorizes the PCNs in light of common network architectures and blockchain types. In Section 4 we define user and business privacy, discuss possible attacks on the privacy of the participants in the PCNs, and present an evaluation of state-of-the-art solutions for what they offer in terms of privacy. Section 5 offers directions about the future research on privacy in PCNs and Section 6 concludes the paper.

2. BACKGROUND

2.1 Blockchain

Blockchain is the underlying technology in cryptocurrency, that brings a new distributed database which is a public, transparent, persistent, and append-only ledger co-hosted by the participants. With various cryptographically verifiable methods, called *Proof-of-X* (PoX), each participant in the network holds the power of moderation of the blockchain [6]. As an example, being the first invented and largest cryptocurrency, Bitcoin and the second largest one, Ethereum, which jointly hold 75% of total market capitalization in the cryptocurrency world, utilize a *proof-of-work* (PoW) mechanism where a participant has to find a "block-hash-value" smaller than a jointly agreed number. A block is an element with a limited size that stores the transaction information. Each block holds the hash of the preceding block which in the long run forms a chain of blocks, called, the blockchain. A block is simply comprised of transactions (data), timestamp, nonce, the hash of the block and the hash of the previous block [1] as shown in Fig. 1. The hash of the transaction is inserted into a Merkle tree which enables users to easily verify whether a transaction is in the block or not. "Who-owns-what" information is embedded in the blockchain as transaction information.

In order for a block to be accepted as valid, the hash of the block should be smaller than a number which is decided by considering the total accumulated computational power in the entire network. By changing the nonce value in the block, the miner aims to find a suitable hash result. Soon after a valid block is found, it gets distributed in the network. After the other nodes validate that block, the next block calculation starts.

Therefore, the cohort of independent participants turns blockchain into a liberated data/asset management technology free of trusted third parties.

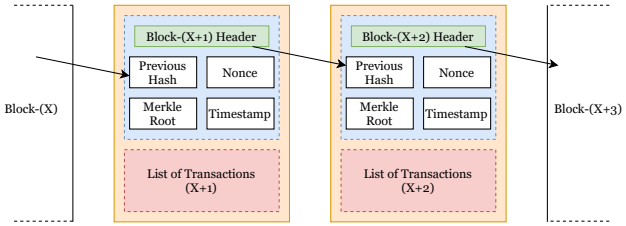

Fig. 1 – Blocks connected with hash.

2.2 Cryptocurrency

Although it finds many areas, the most commonly used application of blockchain technology is cryptocurrencies. A *cryptocurrency* is a cryptographically secure and verifiable currency that can be used to purchase goods and services. In this paper, we will use cryptocurrency and money interchangeably.

Blockchain technology undoubtedly changed the way data can be transferred, stored, and represented. Nonetheless, making a consensus on the final state of a distributed ledger has drawbacks. The first drawback is long transaction confirmation times. For example, in Bitcoin, a block is generated about every 10 minutes. As a heuristic Bitcoin users wait for 6 blocks for the finality of a transaction which yields around 60 minutes of waiting time for finalizing a transaction. In Ethereum, the time between blocks is shorter but users wait 30 consecutive blocks which yield 10-15 minutes of waiting time. Note that, as a block is limited in size, not only the throughput will be limited, but also the total waiting time for the users will be longer during the congested times of the transfer requests. Nevertheless, if a user is in a hurry for approval of a transaction, it will need to pay larger fees to the miners than what its competitors do. This brings us the second drawback of using blockchain for cryptocurrency. The miner nodes, which generate and approve blocks, get fees from the users to include their transactions in blocks. The fee amount is independent of the amount being transacted. During highly congested times, to make a larger profit, miners will be extremely selective in picking the requests from the transaction request pool (*mempool*). So when there is congestion, a payer either has to offer more fees or she/he has to wait more so that a miner picks her/his transaction request.

2.3 Smart contracts

The ability to employ smart contracts is another feature that makes blockchain an unorthodox asset management technology. Smart contracts are scripts or bytecodes, which define how transactions will take place based on

the future events defined within the contract. The joining parties will interact under the defined rules to execute the protocol. It provides mechanisms to embed governance rules in a verifiable way that can be audited by the consensus algorithm. It facilitates a complex procedure that involves several third parties. Smart contracts can be utilized in conditional/unconditional peer-to-peer (P2P) transactions, voting, legal testament, etc. As always, the duty of decision-making is on the blockchain. Hence, the blockchain finalizes the transaction outputs when the smart contracts are utilized too.

3. PCNS AND THEIR CATEGORIZATION

3.1 Payment channel networks

Due to scalability issues researchers have always been in the search for solutions to make the cryptocurrency scalable. Among many offered solutions, the *off-chain* payment channel idea has attracted the most interest.

To establish such a channel, two parties agree on depositing some money in a multi-signature (2-of-2 multisig) wallet with the designated ownership of their share. The multi-sig wallet is created by a smart contract where both parties sign. The smart contract, mediated by the blockchain, includes the participants' addresses, their share in the wallet, and information on how the contract will be honored. Approval of the funding transaction by the blockchain initiates the channel. Afterward, the idea is simple; the payer side gives ownership of some of his/her money to the other side by mutually updating the contract locally. To close the channel the parties submit the final "commitment transaction" to the blockchain for it to honor the final state of the channel. Thus, each side receives its own share from the multi-sig wallet.

The off-chain mechanism brings a huge advantage such that the peers do not need to publish every transaction on the blockchain. That is, the payments are theoretically instantaneous. Moreover, as there is no need for frequent on-chain transactions, the transactions will be protected from fluctuating, unexpectedly high on-chain transaction fees. In fact, a transaction fee can be zero if the peers agree so.

Payment channels created among many parties make the establishment of *multi-hop payments* from a source to a destination through intermediary nodes possible. As shown in, Alice-Charlie (A-C) and Charlie-Bob (C-B) have channels. Let, A-C and C-B are initialized when `time` is `t`. Although Alice does not have a direct channel to Bob, she can still pay Bob via Charlie. At `time` `t+x1`, Alice initiates a transfer of 10 units to Bob. The money is destined to Bob over Charlie. When Charlie honors this transaction in the C-B channel by giving 10 units to Bob, Alice gives 10 units of her share to Charlie in the A-C channel. When the transfers are over, A-C and C-B channel states get updated. When `time` is `t+x2`, Alice makes another transaction (20 units) to Bob and the shares in the channel states get updated once again.

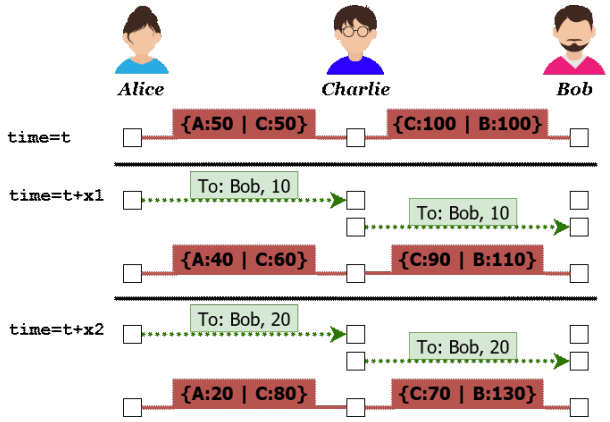

Fig. 2 – A simple multi-hop payment. Alice can initiate a transfer to Bob utilizing channels between Alice-Charlie and Charlie-Bob.

The multi-hop payment concept enables the establishment of a network of payment channels among users, which is referred to as PCN as shown in Fig. 3. A PCN, in essence, is a collection of payment channels. Going back to the example given in Fig. 2, when Alice wants to transfer X units of money to Bob, they have to find a path between each other in which each channel should have a satisfactory directional deposit so that it can handle the transfer of that amount. For incentivizing the intermediary nodes, the responsible parties can pay forwarding fees to the intermediaries. To prevent intermediaries from stealing the funds a cryptographic hash lock protects the money during the traversal. When an intermediary justifies that it knows the hash of the secret, the channel contract honors the transfer. Hence, when Alice initiates a transfer to Bob she will share the secret with Bob in an out-of-bound communication channel. That will let Bob claim the transfer from the preceding node. In return, the node will learn the secret and like a chain reaction, each node will claim the funds from the preceding node until Alice. Current PCNs vary in terms of what topologies they depend on and which Layer-1 blockchain technology they utilize. We discuss this categorization next. We will then explain each of these PCNs in more detail and categorize them in Section 4.

3.2 PCN architectures

In this section, we categorize the types of *network architectures* that can be used in PCNs.

3.2.1 Centralized architecture

In this type of network, there is a central node, and users communicate with each other either over that central node or based on the rules received from the central node as shown in Fig. 4(a). From the governing point of view, if an organization or a company can solely decide on the connections, capacity changes, and flows in the network, then this architecture is called to be a centralized one.

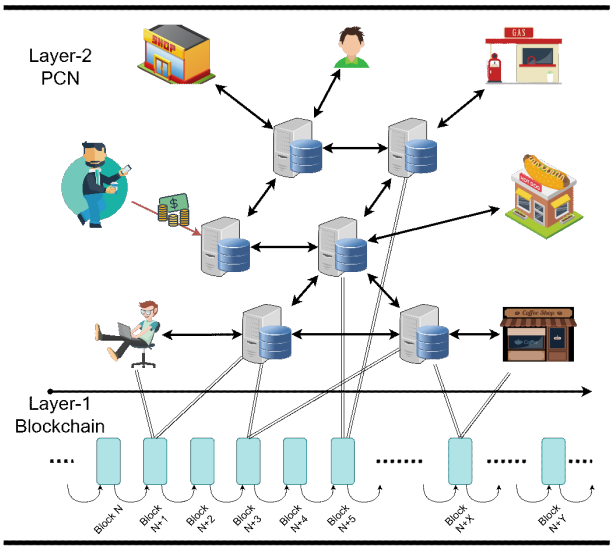

Fig. 3 – The users and businesses independently come together and establish payment channels between each other. Consequently, they form a PCN of end users and relays acting as the backbone. Solid-arrowed lines represent channels between the nodes. Double lines represent how they agreed in the blockchain to establish a channel (only some of these are shown for simplicity).

3.2.2 *Distributed architecture*

In distributed networks, there is no central node. As opposed to the centralized network, each user has the same connectivity, right to connect, and voice in the network. A sample architecture is shown in Fig. 4(b).

3.2.3 *Decentralized architecture*

This type of architecture is a combination of the previous two types which is shown in Fig. 4(c). In this architecture, there is no singular central node, but there are independent central nodes. When the child nodes are removed, central nodes' connections look very much like a distributed architecture. However, when the view is concentrated around one of the central nodes, a centralized architecture is observed.

3.2.4 *Federated architecture*

Federated architecture sounds very much like the federation of the states in the real world and arguably lies somewhere between centralized and decentralized networks. In a federated architecture, there are many central nodes where they are connected in a P2P fashion. Then the remaining nodes (children) strictly communicate with each other over these central nodes which very much looks like a federation of centralized architectures. Moreover, each federation can come up with their local rules in addition to the protocol being used.

3.3 Types of blockchain networks

In this section, we categorize the existing PCNs based on the blockchain type they employ. There are mainly three types of blockchains employed by PCNs.

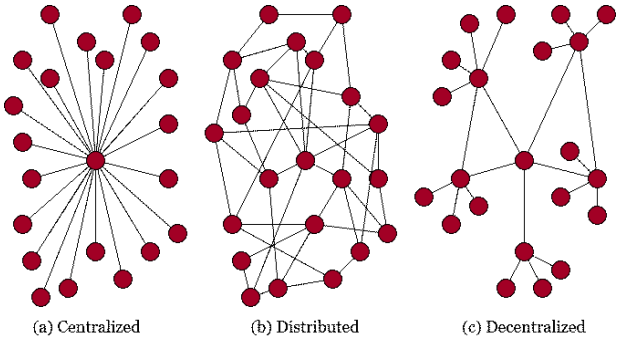

Fig. 4 – Network types

3.3.1 *Public blockchain*

In a public blockchain, no binding contract or registration is needed to be a part of the network. Users can join or leave the network whenever they want. Consequently, the PCN will be open to anyone who would like to use it.

3.3.2 *Permissioned blockchain*

Permissioned (i.e., Private) blockchain lays on the opposite side of the public blockchain, where the ledger is managed by a company/organization. Moreover, the roles of the nodes within the network are assigned by the central authority. Not everybody can participate or reach the resources in the permissioned blockchain. PCNs employing permissioned blockchain will be "members-only".

3.3.3 *Consortium blockchain*

Contrary to the permissioned blockchain, in consortium blockchain, the blockchain is governed by more than one organization. From the centralization point of view, this approach seems more liberal but the governance model of the blockchain slides it to the permissioned side. PCNs utilizing consortium blockchain will be similar to permissioned blockchain in terms of membership but in this case, members will be approved by the consortium.

4. PRIVACY ISSUES IN PCNS: METRICS AND EVALUATION

As PCNs started to emerge within the last few years, a lot of research has been devoted to making them efficient, robust, scalable, and secure. However, as some of these PCNs started to be deployed, they reached a large number of users (e.g., LN has more than 10K users), which is expected to grow further as long as users are satisfied with their services. Such growth brings several privacy issues that are specific to PCNs. In this respect, we observed that strengthening the security in PCNs comes with weaker privacy while strengthening the privacy in PCN makes the network less practical. We argue that very little attention has been paid to these issues and there is a need to identify and understand privacy risks in PCNs from both the users' and businesses' perspectives. Therefore, in this section, we first define these privacy metrics and explain

possible privacy attacks in PCNs. We then summarize the existing PCNs to evaluate their privacy capabilities concerning these metrics for the first time. Our goal is to increase awareness to not only strengthen the privacy features of the existing PCNs but also help designers to consider the privacy-by-design principle when creating new PCNs from scratch. Next, we summarize the state-of-the-art PCN proposals.

4.1 Privacy in PCNs

In its simplest form, *data privacy* or *information privacy* can be defined as the process which answers how storage, access, and disclosure of data take place. For centrally managed systems the central node (or company) is the responsible party for preserving the privacy of the users by defining appropriate policies to manage their data. However, when the system shifts towards a decentralized/distributed one, the privacy of the users should be taken care of by the protocol running beneath the network.

For instance, Bitcoin aims to keep the real identities private utilizing pseudonyms. It is seen that inherited from this philosophy, PCN designers also pay attention to privacy features with different points of view. Nevertheless, we observe that strengthening the security in PCN comes with weaker privacy or strengthening privacy makes the network less practical. The PCN needs to provide services ensuring that the users' data will not be exposed without their authorization. However, the user data travels within the PCN through many other users. Hence, to assess the level of privacy in a particular decentralized system, definitions for privacy within the system are needed. To address these issues, some PCN works aimed to hide the sender (u_s) or the receiver (u_r) identity (i.e., *anonymity*) whereas some others concentrated on strengthening the *relationship anonymity* between the sender and the recipient.

4.2 Attack model and assumptions

There are two types of attackers considered in this paper. The first attacker is an *honest-but-curious* (HBC) where the attacker acts honestly while running the protocols but still collects information passively during operations. The second attacker of interest is the *malicious* attacker that controls more than one node in the network to deviate from the protocols. Hence, it can act based on its own rules, e.g. denial of service or colluding with other nodes in order to learn about the user/payment information. For both of the attacker types, the attacker either tries to learn the origin and the destination of the payment or tries to learn the path of the payment routing. This information can be used for a couple of purposes. The first purpose of trying to get this information is censoring the payment by simply rejecting it. The second purpose is trying to guess the business capacity of a node. The third reason is trying to learn the spending habits of the customers. If a single item is purchased, a persistent attacker will be able to relate the payment to the service or good that has been purchased. The fourth purpose is trying to discredit a particular node simply by slowing down the transaction so that the customers will tend to lose interest in that seller because of a lack of payment usability. These attacker types and how they can situate in the network are shown in Fig. 5 as follows: ① The attacker is on the path of a payment. ② The attacker is not on the path of a particular payment but it can partially observe the changes in the network. ③ The attacker colludes with other nodes, for example, to make packet timing analysis with sophisticated methods.

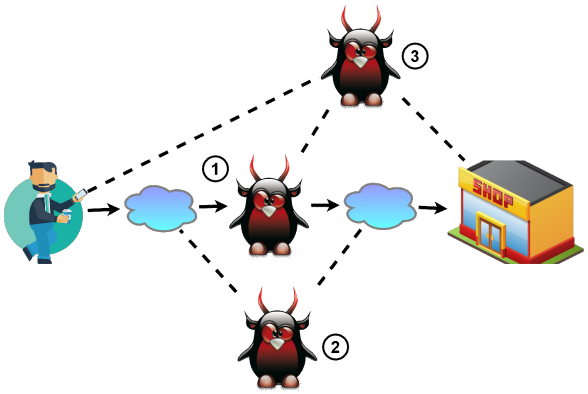

Fig. 5 – Attackers can appear in the network in different places.

Based on these assumptions, we consider the following potential attacks for compromising privacy in PCNs:

- **Attacks on Sender/Recipient Anonymity**: Sender/Recipient anonymity requires that the identity of the sender/recipient (u_s/u_r) should not be known to the others during a payment. This is to protect the privacy of the sender/recipient so that nobody can track their shopping habits. There may be cases where an adversary may successfully guess the identity of the sender/recipient as follows: For case ①, the sender can have a single connection to the network, and the next node is the attacker, hence, the attacker is sure that u_s is the sender. For case ② the attacker may guess the sender/recipient by probing the changes in the channel balances. For case ③ the attacker will learn the sender/recipient if it can carry out a payment timing analysis within the partial network formed by the colluded nodes.
- **Attack on Channel Balance Privacy.** To keep the investment power of a user/business private, the channel capacities should be kept private in PCNs. The investment amount in a channel would give hints about the financial situation of a user or its shopping preferences. Moreover, if the capacity changes in the channels are known, tracing them causes indirect privacy leakages about the senders/recipients. For instance, an attacker can initiate fake transaction requests. After gathering responses from intermediary nodes, it can learn about the channel capaci-

ties. This attack is not necessarily about depleting the channel capacities but guessing the channel capacity of a node. Continuously learning the channel capacities will eventually yield more complicated privacy attacks as discussed in the attack on sender privacy.

- **Relationship Anonymity.** In some cases identities of u_s or u_r may be known. This is a very valid case for retailers because they have to advertise their identities to receive payments. However, if an attacker can relate the payer to the payee, not only the spending habits of the sender but also the business model of the recipient will be learned. In such cases, the privacy of the trade can be preserved by hiding the relationship between the sender and recipient. Specifically, who-pays-to-whom information should be kept private. Some of the PCNs utilize onion-routing to forward the transactions to the destination node. Onion-routing is a source-routing protocol where the source of a message encapsulates the data with the keys of the intermediary nodes like a stacking doll. An intermediary node can remove only one layer from the incoming message to see the next node to which the data is to be forwarded. Hence, in a distributed network, an intermediary node will not confidently be aware of who talks to whom.

- **Business Volume Privacy.** For a retailer, publicly disclosed revenue will yield the trade secrets of its business, which must be protected by the PCN. In that sense, the privacy of every payment is important. Such payment privacy can be attacked as follows: In a scenario where two or more nodes collude, the amount of a transaction can be known to the attacker. In another scenario, if the recipient is connected to the network via a single channel through the attacker, then it will track all of the flows towards the recipient.

4.3 State-of-the-art PCNs and their privacy evaluation

In this section, we briefly describe current studies that either present a complete PCN or propose revisions to the current ones, then analyze their privacy capabilities based on our threat model. We provide a summary of the assessment of the current PCNs' categorizations and privacy features in Table 1. Although our main interest in this paper is specifically payment channel networks, for privacy in permissionless blockchains, the readers are advised to have a look at [7].

4.3.1 Lightning network (LN)

LN [4] is the first deployed PCN that utilizes Bitcoin. It started in 2017 and by June 2020 serves with more than 12.000 nodes and 36.000 channels. Nodes in LN utilize *"Hashed Time-Locked Contracts"* (HTLC) for multi-hop transfer. The directional capacities in the payment channels are not advertised but the total capacity in the channel is known for a sender to calculate a path. This provides a partial channel balance privacy. The sender encrypts the path by using the public keys of the intermediary nodes by utilizing *"onion-routing"* so that the intermediary nodes only know the addresses of the preceding and the following nodes. None of the intermediary nodes can guess the origin or the destination of the message by looking at the network packet.

4.3.2 Raiden network

Shortly after LN, Ethereum foundation announced Raiden Network [5]. Raiden is the equivalent of LN designed for transferring Ethereum ERC20 tokens and provides the same privacy features. Although Ethereum is the second-largest cryptocurrency, that popularity is not reflected well in the Raiden Network. As of June 2020, Raiden serves with 25 nodes and 54 channels. The advantage of Raiden over LN is, due to tokenization, users can generate their own tokens to create a more flexible trading environment.

4.3.3 Spider network

Spider network [16] is a PCN that proposes applying packet-switching based routing idea which is seen in traditional networks (e.g., TCP/IP). However, it is known that in packet-switching the source and the destination of the message should be embedded in the network packet. The payment is split into many micro-payments so that the channel depletion problem gets eliminated. The authors also aimed to have better-balanced channels. In this PCN, there are *spider routers* with special functionalities that communicate with each other and know the capacities of the channels in the network. The sender sends the payment to a router. When the packet arrives at a router, it is queued up until the funds on candidate paths are satisfactory to resume the transaction. The authors do not mention privacy and plan to utilize onion-routing as a future work. The micro-payments might follow separate paths, which would help to keep business volume private if the recipients were kept private. Additionally, the hijack of a router will let an attacker learn everything in the network.

4.3.4 SilentWhispers

SilentWhispers [9] utilizes landmark routing where landmarks are at the center of the payments. In their attack model, either the attacker is not on the payment path or a landmark is HBC. Here, landmarks know the topology but they do not know all of the channel balances. When the sender wants to send money to a recipient, she/he communicates with the landmarks for her/his intent. Then landmarks start communicating with the possible nodes from "sender-to-landmark" to the "landmark-to-recipient" to form a payment path. Each node in the

Table 1 – Qualitative evaluation of privacy features of existing PCNs.

	Network Type	Blockchain Type	Sender Anonymity	Recipient Anonymity	Channel Balance Privacy	Relationship Anonymity	Business Volume Privacy
Lightning Network (HTLC) [4]	Decentralized/ Distributed	Public	◑	◑	◑	◑	●
Raiden Network [5]	Decentralized/ Distributed	All	◑	◑	◑	◑	●
Spider [8]	Decentralized/ Centralized	All	◑	◑	○	◑	◑
SilentWhispers [9]	Decentralized/ Centralized	All	◑	◑	◑	◑	◑
SpeedyMurmurs [10]	Decentralized/ Centralized	Public	◑	◑	◑	◑	◑
PrivPay [11]	Decentralized/ Centralized	Permissioned	◑	◑	◑	◑	◑
Bolt [12]	Centralized	Public	●	●	●	●	●
Fulgor [13]	Decentralized/ Distributed	Public	●	●	◑	●	●
Rayo [13]	Decentralized/ Distributed	Public	◑	◑	◑	◑	●
Erdin et al. [14]	Distributed/ Federated	All	◑	●	◑	◑	●
Anonymous Multi-Hop Locks (AMHL) [15]	Decentralized/ Distributed	Public	○	●	◑	●	●

◑: Partially satisfies OR can not defend against all mentioned attacks.
●: Fully satisfies.
○: Does not satisfy.

path discloses the channel balance availability for the requested transfer amount to the landmarks. Then landmarks decide on the feasibility of the transaction by doing multi-party computation. During the transfer phase, when an intermediary node realizes the transaction to the next node, it informs the landmark. Landmarks acknowledge the transactions and when all of the transactions are executed on the intended path, the transaction is marked successful. In SilentWhispers, the sender and the receiver are kept private but the landmarks know the sender-recipient pair. The payment amount is also private for the nodes who do not take part in the transaction. Moreover, the balances of the channels within the network are kept private. Although centralization is possible, the approach is decentralized and landmarks are trusted parties.

4.3.5 SpeedyMurmurs

SpeedyMurmurs [10] is a routing protocol, specifically an improvement for LN. In SpeedyMurmurs, there are well-known landmarks like in SilentWhispers. The difference of this approach is that the nodes on a candidate path exchange their neighbors' information anonymously. So if a node is aware of a path closer to the recipient, it forwards the payment in that direction, called "shortcut path". In a shortcut path, an intermediary node does not necessarily know the recipient but knows a neighbor close to the recipient. SpeedyMurmurs hides the identities of the sender and the recipient by generating anonymous addresses for them. Intermediary nodes also hide the identities of their neighbors by generating anonymous addresses. Although it may be complex, applying de-anonymization attacks on the network will turn it into SilentWhispers. This is because, while the algorithm is a decentralized approach, with unfair role distribution, it may turn into a centralized approach.

4.3.6 PrivPay

PrivPay [11] is a hardware-oriented version of SilentWhispers. The calculations in the landmark are done in tamper-proof trusted hardware. Hence, the security and privacy of the network are directly related to the soundness of the trusted hardware which may also bring centralization. In PrivPay, sender privacy is not considered. Receiver privacy and business volume privacy is achieved by misinformation. When an attacker constantly tries to query data from other nodes the framework starts to produce probabilistic results.

4.3.7 Rayo and Fulgor

: Rayo and Fulgor [13] are two multi-hop routing protocols for PCNs (Fulgor is suitable for LN only). They develop these protocols against the security flaw coming from hash distribution in LN. Specifically, the same hash of the pre-image is distributed on the path when a payment takes place so the authors argue that this creates a problem for the privacy and relationship anonymity between the sender and the recipient. To solve that problem they introduce multi-hop HTLC contracts. In their non-blocking approach, Rayo a non-blocking payment routing, there is a global payment identifier system that helps the nodes to order the payments with respect to their identifier number. For that reason, Rayo is prone to relationship anonymity attacks if the attacker is located on the payment path. Fulgor aims for guaranteed privacy. The multi-hop HTLC contract offered in Fulgor is fully compliant with the Bitcoin scripts. Thus, it is only usable in LN or Bitcoin-like cryptocurrency backed PCNs. Fulgor's motivation is that in LN the same hash of the pre-image is distributed on the payment path. This creates a privacy problem which by comparing the collected hashes colluding nodes can learn about the path of the payment. Fulgor introduces one more phase of messaging with zero-knowledge proof-based communication. The sender distributes unique hashes to the intermediary nodes. It satisfies balance privacy, business privacy, sender and recipient anonymity.

4.3.8 Bolt

Bolt [12] is a hub-based payment system. That is, there is only one intermediary node between the sender and recipient. Bolt assumes *zero-knowledge proof*-based cryptocurrencies. It does not satisfy privacy in multi-hop payments, however, it satisfies very strong relationship anonymity if the intermediary node is honest. On the other hand, being dependent on a single node makes this approach a centralized one.

4.3.9 Permissioned Bitcoin PCN

In PCNs, if the network topology is not ideal, e.g., star topology, some of the nodes may learn about the users and payments. To this end, the authors in [14] propose a new topological design for a permissioned PCN such that the channels' depletion can be prevented. They come up with a real use case where a consortium of merchants create a full P2P topology and the customers connect to this PCN through merchants which undertakes the financial load of the network to earn money. The privacy of the users in the PCN is satisfied by LN-like mechanisms. The authors also investigate how initial channel balances change while the sender/receiver privacy and the relationship anonymity can be satisfied by enforcing at least 3-hops in a multi-hop payment.

4.3.10 Anonymous Multi-Hop Locks (AMHL)

In the AMHL proposal [15], the authors offer a new HTLC mechanism for PCNs. On a payment path, the sender agrees to pay a service fee to each of the intermediaries for their service. However, if two of these intermediaries maliciously collude they can eliminate honest users in the path and consequently steal their fees. In order to solve this, they introduce another communication phase

in which the sender distributes a one-time-key to the intermediary nodes. Although the HTLC mechanism is improved for the security of the users the sender's privacy is not protected; each of the intermediaries learns the sender. However, relationship anonymity can still be satisfied.

5. FUTURE RESEARCH ISSUES IN PCNS

Privacy in PCNs is an understudied topic and many open issues need to be addressed as future research. In this section, we summarize these issues:

Abuse of the PCN protocols. Most of the PCNs rely on public cryptocurrencies, whose protocol implementations are public. This freedom can be abused such that by changing some parameters and algorithms in the design, an attacker can behave differently than what is expected. This will bring privacy leakages and censorship to the network. A topological reordering of the network will help solve this problem. If a sender gets suspicious about an intermediary node, it can look for alternatives instead of using that node.

PCN topologies. The most widely accepted and readily available solution, Lightning Network, has a user base of more than 12 thousand nodes as of today. Furthermore, if the channels are observed it creates an impression that most of the nodes are experimental to discover the capabilities of LN. Even the trust in the protocol becomes perfect, assuming that ordinary users will put hundreds of dollars in their channels as collateral does not make perfect sense. This reality reminds us that PCNs are inclined to slide towards centrally managed networks. In that case, topology formation comes into the scene. Right now, the `autopilot` feature of `lnd` (an LN client) highlights a scale-free Barabasi-Albert network formation method. However, this method does not take the financial strength of the attendees but only their existence.

Discovery of Colluding Nodes. When the nodes collude in a PCN, they can extract more information about the users. To prevent this, the protocols should be enriched to discover the colluding nodes or by adding redundancy to the protocols, colluding nodes can be confused.

Policy Development. The cryptocurrency and PCN idea is still in the early phases of their lives. Hence, policy and regulation for not only the security of the participants but also for the privacy of them are highly needed in this domain. This will also create a quantitative metric for the researchers to measure the success of their proposals.

Impact of Scalability on Privacy. One of the aims for introducing PCNs was making the cryptocurrencies more scalable. For example, LN advises running the Barabasi-Albert scale-free network model while establishing new connections [17]. Thus, the final state of the network can impose centralization which will have adverse effects on the privacy of the nodes in the network.

Integration of IoTs with PCNs. Use of IoT devices for payments are inevitable. Aside from the fact that most IoT devices are not powerful to run a full node, the security and privacy of the payments and the device identities within the IoT ecosystem need to be studied. These devices are anticipated to be able to participate in the network through gateways. The revelation of device ownership will reveal the real identity of the users to the public which is a big threat to privacy.

Privacy in Permissioned PCNs. While establishing a network of merchants in permissioned PCNs, the merchants should at least disclose their expected trade volume in order to establish a dependable network. This will, however, yield trade secrets of the merchants. To prevent this, zero-knowledge proof based multi-party communication can be explored.

6. CONCLUSION

PCN is a promising solution to make cryptocurrency-based payments scalable. This idea aimed to fix two major shortcomings of cryptocurrencies: long confirmation times and high transaction fees. There are many studies on the design of payment channels and PCNs to make the transfers secure and efficient. However, these studies do not mention the possible privacy leakages of these methods in case of a wide adaptation of proposed ideas. In this paper, we first made the categorization of PCNs based on the type of blockchain being used and the topological behavior of the network. After clearly defining possible privacy leakages in a PCN, we compared and contrasted the state-of-the-art PCN approaches from the privacy point of view.

REFERENCES

[1] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu, and Richard Brooks. A brief survey of cryptocurrency systems. In *2016 14th annual conference on privacy, security and trust (PST)*, pages 745–752. IEEE, 2016.

[3] Florian Tschorsch and Björn Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 18(3):2084–2123, 2016.

[4] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016.

[5] Raiden Network: Fast, cheap, scalable token transfers for Ethereum. https://raiden.network/. Accessed: 2020-06-06.

[6] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn,

and George Danezis. Sok: Consensus in the age of blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, pages 183–198, 2019.

[7] Li Peng, Wei Feng, Zheng Yan, Yafeng Li, Xiaokang Zhou, and Shohei Shimizu. Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks*, 2020.

[8] Vibhaalakshmi Sivaraman, Shaileshh Bojja Venkatakrishnan, Mohammad Alizadeh, Giulia Fanti, and Pramod Viswanath. Routing cryptocurrency with the spider network. *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*, pages 29–35, 2018.

[9] Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, and Matteo Maffei. Silentwhispers: Enforcing security and privacy in decentralized credit networks. In *The Network and Distributed System Security (NDSS)*, 2017.

[10] Stefanie Roos, Pedro Moreno-Sanchez, Aniket Kate, and Ian Goldberg. Settling payments fast and private: Efficient decentralized routing for path-based transactions. *arXiv preprint arXiv:1709.05748*, 2017.

[11] Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, and Kim Pecina. Privacy preserving payments in credit networks. In *Network and Distributed Security Symposium*, 2015.

[12] Matthew Green and Ian Miers. Bolt: Anonymous payment channels for decentralized currencies. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 473–489, 2017.

[13] Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, and Srivatsan Ravi. Concurrency and privacy with payment-channel networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 455–471, 2017.

[14] Enes Erdin, Mumin Cebe, Kemal Akkaya, Senay Solak, Eyuphan Bulut, and Selcuk Uluagac. A bitcoin payment network with reduced transaction fees and confirmation times. *Computer Networks*, page 107098, 2020.

[15] Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. Anonymous multi-hop locks for blockchain scalability and interoperability. In *NDSS*, 2019.

[16] Vibhaalakshmi Sivaraman, Shaileshh Bojja Venkatakrishnan, Mohammad Alizadeh, Giulia Fanti, and Pramod Viswanath. Routing cryptocurrency with the spider network. In *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*, pages 29–35, 2018.

[17] Stefano Martinazzi and Andrea Flori. The evolving topology of the lightning network: Centralization, efficiency, robustness, synchronization, and anonymity. *Plos one*, 15(1):e0225966, 2020.

AUTHORS

Enes Erdin is an Assistant Professor at the University of Central Arkansas. He got his Ph.D. in the Department of Electrical and Computer Engineering at Florida International University and he was an NSF CyberCorps Fellow. He conducts research in the areas of hardware security, blockchain technology, and Cyber-physical Systems.

Suat Mercan is a postdoctoral researcher at Florida International University. He received his Ph.D. degree in Computer Science at the University of Nevada, Reno in 2011 and his M.S degree in Electrical and Computer Engineering from the University of South Alabama in 2007. His main research interests are blockchain, payment channel and peer-to-peer networks, cybersecurity, digital forensic, and content delivery.

Kemal Akkaya is a professor in the Department of Electrical and Computer Engineering at Florida International University. He leads the Advanced Wireless and Security Lab and is an area editor of the Elsevier Ad Hoc Networks Journal. His current research interests include security and privacy, and protocol design. He has published over 120 papers in peer-reviewed journals and conferences. He received the “Top Cited” article award from Elsevier in 2010.