Privacy-Utility Tradeoffs in Routing Cryptocurrency over Payment Channel Networks

Weizhao Tang
Carnegie Mellon University
wtang2@andrew.cmu.edu

Weina Wang
Carnegie Mellon University
weinaw@cs.cmu.edu

Giulia Fanti
Carnegie Mellon University
gfanti@andrew.cmu.edu

Sewoong Oh
University of Washington
sewoong@cs.washington.edu

CCS CONCEPTS

• **Security and privacy → Privacy-preserving protocols**; • **Networks → Network privacy and anonymity**; *Network algorithms.*

KEYWORDS

Blockchain, privacy, p2p network

ACM Reference Format:
Weizhao Tang, Weina Wang, Giulia Fanti, and Sewoong Oh. 2020. Privacy-Utility Tradeoffs in Routing Cryptocurrency over Payment Channel Networks. In *ACM SIGMETRICS / International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS '20 Abstracts), June 8–12, 2020, Boston, MA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3393691.3394213

1 INTRODUCTION

As the adoption of cryptocurrencies grows to unprecedented levels, the scalability of blockchain technologies has become increasingly important. A major open question is whether cryptocurrencies are fundamentally able to support as much traffic as traditional, centralized solutions. One prominent approach for improving the scalability of blockchains is *payment channel networks* (PCNs) [1]. Instead of committing every transaction to the blockchain, a separate overlay network (called a PCN) is maintained. Each node represents a user, and each edge (or *payment channel*) represents pre-allocated funds that can be efficiently transacted between the two endpoints under a mutual agreement. Users can transact with each other by relaying payments over a sequence of channels.

A major challenge in deploying PCNs in real-world cryptocurrencies is the tension between throughput and privacy. Each time a user wishes to route a transaction, it must find a path through the PCN with enough pre-allocated funds to support the transaction. However, in today's PCNs, edge balances are not publicly revealed for privacy reasons. This causes failed routing attempts, thereby decreasing the transaction throughput of the system and ultimately hindering scalability. The goal of this paper is to quantify this tradeoff between privacy and utility in PCNs.

SIGMETRICS '20 Abstracts, June 8–12, 2020, Boston, MA, USA

ACM ISBN 978-1-4503-7985-4/20/06.
https://doi.org/10.1145/3393691.3394213

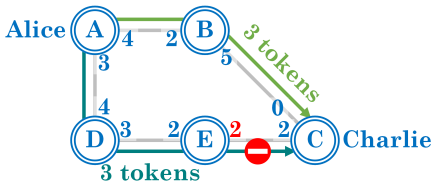

Figure 1: Payment channel network. Alice tries to send 3 tokens to Charlie. The bottom route fails because edge (E, C) does not have sufficient balance in the $E \to C$ direction.

Payment Channel Networks (PCNs). A *payment channel* is a transaction between two parties that escrows currency for use only between those two parties for some amount of time. Once the channel is finalized, the parties can send escrowed funds back and forth by digitally signing the previous state of the channel and the new updated transaction. When the parties decide to close the channel, they can commit its final state through another blockchain transaction. A *payment channel network* (PCN) sets up a graph of bidirectional payment channels. The key idea is that if Alice wants to transact with Charlie, but is only connected to him via Bob, then Bob can act as a relay for Alice's money, passing it along to Charlie (for a small routing fee). Notice that if Alice wants to send r tokens to any node in the network, she must first find a directed path to that node with at least r tokens on every (directed) edge.

Today's PCNs do not reveal instantaneous balance information in an attempt to prevent observers from inferring other users' transaction patterns. Thus, PCN users know the graph topology, but are forced to guess if a given path has enough balance to support a particular transaction by attempting to send their transaction over that path. This guess-and-check routing approach uses unnecessary resources and severely limits the success rates of today's PCNs [2]. We want to understand whether privacy must always come at a high cost of transaction success rate. In particular, we consider whether a system could reveal partial, randomized channel balances in an effort to gracefully trade off privacy for utility.

Contributions. Our contributions are fourfold:

- We theoretically model the routing problem in PCNs and define distribution-free metrics for privacy and utility. In particular, we relate the *success rate* of a scheme, or the fraction of successfully routed transactions, to a simplified but analytically tractable quantity we call *utility*.

- We show a restrictive, so-called *diagonal* upper bound on the privacy-utility tradeoff for these metrics over general graphs and a significant class of shortest-path transaction routing strategies. We show that the diagonal bound is tight by designing noise mechanisms that achieve it.
- The diagonal bound is a somewhat negative result, suggesting that a good tradeoff is not possible. However, we show that by relaxing certain assumptions (e.g., the shortest-path routing assumption), we can break the diagonal barrier. Indeed, one can design noise mechanisms that asymptotically achieve a perfect privacy-utility tradeoff. However, this comes at the cost of increasingly long paths, i.e., increasingly expensive routing fees.
- We demonstrate through simulation that even if one were to consider an average-case utility metric (fraction of successful transactions, or success rate) rather than a worst-case one, the privacy-success rate tradeoff is still not favorable for shortest-path routing. Overall, our simulations suggest that trading off privacy for utility does not give significant gains unless the system operates either in a low-privacy regime or low-utility regime; today's PCNs operate in the low-utility regime.

In sum, our results suggest that PCNs may not be able to provide utility and privacy simultaneously. Moreover, our theoretical analysis is conducted under an adversarial model that (a) is passive, and (b) does not exploit temporal correlations in transaction patterns. Hence, actual privacy threats are likely even more dire than our results indicate. PCN system designers may therefore need to make an explicit choice regarding whether the value of PCNs comes mainly from their potential for improving performance or privacy, and choose an operating point accordingly.

2 MAIN RESULTS

We model the PCN as a graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ denotes participating nodes with $n = |\mathcal{V}|$, and $\mathcal{E}$ the payment channels. Each edge $(u, v) \in \mathcal{E}$ is associated with two weights, b_{uv} and b_{vu}, which denote the balances from u to v and from v to u, respectively. These true balances are not necessarily equal to the publicly-released channel balances, which we denote by $\tilde{b}_{uv}$ and $\tilde{b}_{vu}$, respectively.

We assume an arbitrary sequence of transactions enters the system sequentially. For a path P on the graph, we use $s(P)$ and $d(P)$ to denote its source and destination, respectively. At arrival of each transaction of value r from source s to destination d, s chooses a path P from s to d on the network, such that $\forall (u, v) \in P$, $\tilde{b}_{uv} \geq r$. The transaction fails if and only if P does not exist, or does not have enough balance. If it fails, there will be no retry or balance update. Otherwise, the true channel balance is updated as $b_{uv} := b_{uv} - r$ and $b_{vu} := b_{vu} + r, \forall (u, v) \in P$. The visible channel balances are updated according to a *noise mechanism* (or *mechanism*). Given an input path P, it outputs a random set of edges $Q \subseteq P$ such that $\forall (u, v) \in Q$, the public balance $\tilde{b}_{uv}$ is updated to the true new balance, b_{uv}. We denote this conditional probability distribution by $\mathbb{D}[Q|P]$.

Privacy metric. Our adversary is an honest-but-curious user that passively observes the network and tries to infer the source and destination of the first transaction to pass through the system. Once the transaction has been processed, it guesses one node $v \in \mathcal{V}$ with probability $\mathbb{A}[v|Q]$, where $\mathbb{A}$ is a randomized adversarial strategy. Privacy is defined as the minimax probability that this adversary makes a wrong estimation (i.e., does not identify the source *or* destination node correctly).

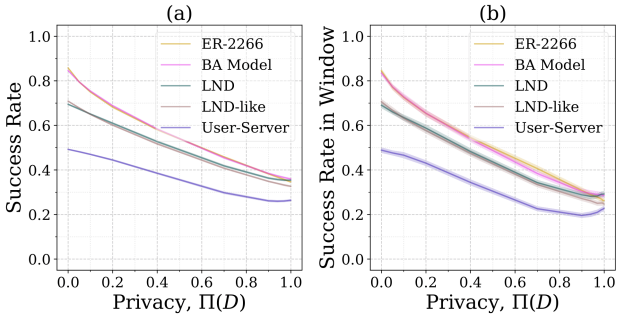

Figure 2: Success rate-privacy curves on different network topologies. Success rate is the fraction of successful transactions out of total 100,000, while "success rate in window" is the fraction out of 2,000 most recent transactions. Higher privacy metric indicates stronger privacy guarantees.

$$\Pi(\mathbb{D}) = 1 - \sup_{\mathbb{A}} \min_{P \in \mathcal{P}} \sum_{Q \subseteq P} \mathbb{D}[Q|P] \sum_{v \in \{s(P), d(P)\}} \mathbb{A}[v|Q]. \quad (2.1)$$

Utility metric. We define the quantity in (2.2) below as the utility of mechanism $\mathbb{D}$. This quantity equals the minimum probability that observed balance of a channel equals the true balance.

$$U(\mathbb{D}) = \min_{P \in \mathcal{P}} \min_{\varepsilon \in P} \sum_{Q : Q \ni \varepsilon, Q \subseteq P} \mathbb{D}[Q|P]. \quad (2.2)$$

Fundamental limits on privacy-utility tradeoff.

Theorem 2.1 (The Diagonal Bound). *On a general network $(\mathcal{V}, \mathcal{E}, \mathcal{P})$ with $n = |\mathcal{V}| \geq 2$, if $\mathcal{P}$ includes only shortest paths, then for any noise mechanism $\mathbb{D}$, its privacy $\Pi(\mathbb{D})$ and utility $U(\mathbb{D})$ satisfy*

$$\Pi(\mathbb{D}) \leq \left(1 - \frac{2}{n}\right)[1 - U(\mathbb{D})]. \quad (2.3)$$

It can be shown that the bound in Theorem 2.1 is made tight by the *all-or-nothing* noise mechanism defined below.

Definition 2.2. For a transaction routed over path P, the **all-or-nothing noise mechanism** $\mathbb{D}_{\mathbf{N}}$ either truthfully updates balance on every edge of P with probability $U(\mathbb{D}_{\mathbf{N}})$, or updates nothing with probability $1 - U(\mathbb{D}_{\mathbf{N}})$.

Simulations. Figure 2 shows privacy-success rate tradeoff curves on different typical network topologies. These curves suggest that sacrificing some amount of privacy gives disproportionately small gains in success rate. In addition, they could be non-monotonic at nearly perfect privacy, which shows sacrificing privacy can actually *reduce* success rate.

REFERENCES

[1] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016.
[2] Neel Varshney. Lightning network has 1 percent success rate with transactions larger than $200, controversial research says. *Hard Fork*, June 2018.