Improving the Anonymity of Blockchains:The Case of Payment Channel Networks with Length-bounded Random Walk Insertion

Mehmet Emre Ozkan (m.e.ozkan@student.tudelft.nl), Satwik Prabhu Kumble (s.prabhu@tudelft.nl), Stefanie Roos (s.roos@tudelft.nl)

Summary

The LND routing is currently the most popular routing algorithm used in the Lightning Network, the second layer solution to Bitcoin's scalability. Despite its popularity, recent studies demonstrate that its deterministic nature compromises the anonymity of the Lightning Network. In other words, threatening parties present in the transaction path can guess the sending and receiving parties of transactions easier than in the absence of such strong determinism.

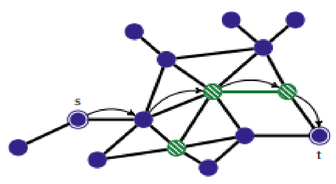
- As a solution, we propose augmenting the LND with a length bounded random walk insertion to include randomness into the transaction path and regain anonymity.
- In simulations with LND routing, attackers could identify senders or receivers for 70% of transactions.
- For simulations of networks with 100 nodes and an average of 2 edges per node with the weighted random walk insertion, attackers could identify senders or receivers around 65% of the time.
- However, for simulations of networks with 500 nodes and an average of 10 edges per node with the weighted random walk insertion, attackers could never identify senders or receivers.
- For the snapshot simulation, they could only identify either in around 4% of transactions. Thus, we overall believe that the random walk insertion into the LND algorithm addresses the anonymity issue of the unmodified algorithm.

Introduction

Research Question: Could we improve the anonymity of blockchains in the case of payment channel networks with length-bounded random walk insertions?

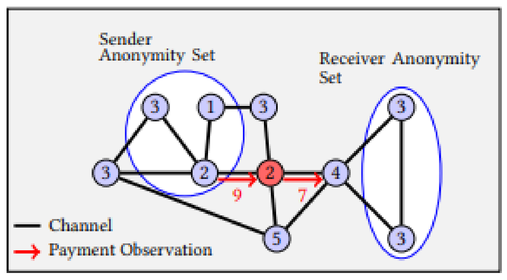
- The Lightning Network is a second-layer solution to Bitcoin's scaling problem. Bitcoin's bottleneck is mainly the number of transactions that can be stored on the blockchain at any given moment. The Lightning Network, a payment channel network, tackles this issue by eliminating the requirement for each transaction to be stored on the blockchain.
- Payment channel network looks like figure 1, each node being a person and each connection being some locked up amount of bitcoin to be used in transactions.

Figure 1:



- The loss in anonymity is created because of two main information available. One of them being publicly available timelocks, which gives information about how much it has left for a transaction. The other one is the routing algorithm, attacking nodes don't know what routing algorithm is used in transactions. But since around 92% of the users use LND routing [1], the attacking node can guess many of the sender's and receiver's, because it is a highly deterministic routing algorithm.

Figure 2:



- A random walk algorithm is a path created completely by random hops from one node to another.

Methodology

- Random Hop insertion algorithms chooses a random node in the optimum path, then from that node performs a random hop, then takes the optimum route again.
- Random Walk insertion algorithm works in a way that it chooses a random node and then performs a random walk from that node by the given length. Then the most optimum route to the target will be taken with LND.
- Weighted Random Walk insertion algorithm works in the same way as Random Walk insertion only difference being the random walk being weighted by the degrees of the nodes.
- After testing against the existing attack from previous research[1] with the generated network while using weighted random walk insertion algorithm around 16% of the transactions had an identifiable sender or receiver compare to 65% with LND routing.
- As the existing attack didn't perform well against the new routing algorithm. An attack against the weighted random walk insertion routing was created.
- The modified attack creates a list of possible senders and receivers, and then generates possible paths for every pair of possible sender, receiver with the weighted random walk insertion algorithm. From the generated paths most popular path that includes the attacking node is chosen as a guess.

Evaluation

Table 1: Attack on Weighted Random Walk Insertion routing algorithm with different lengths, attackers knowing the length. Generated network has 100 nodes with 2 connections per node and 10% attackers.

Parameter	length 2	length 3	length 4	length 10
Singular possible sender/receiver sets	0.39%	0.0%	0.0%	0.0%
Average number of hops	5.18	5.83	7.12	11.43
Average fee	2.26	2.39	3.42	5.57
Average possible sender size	12.63	14.09	15.16	18.00
Average possible receiver size	5.46	4.54	3.57	1.93
An attacker finding either	38.22% ±9.52%	26.73% ±8.67%	21.80% ±8.09%	10.36% ±5.97%
Attackers finding either	61.17% ±9.55%	69.72 ±9.00%	64.42% ±9.38%	56.73% ±9.71%

Table 2: Attack on Weighted Random Walk Insertion routing algorithm with different lengths, attackers don't know the right length. "g" is the length used by attackers. Generated network has 100 nodes with 2 connections per node and 10% attackers.

Parameter	length 2, g = 3	length 3, g = 2	length 4, g = 2	length 10, g = 4
Singular possible sender/receiver sets	0.36%	0.0%	0.0%	0.0%
Average number of hops	5.31	6.35	7.60	11.43
Average fee	2.31	2.69	3.40	5.56
Average possible sender size	13.53	16.67	15.71	18.00
Average possible receiver size	5.29	4.15	3.54	1.93
An attacker finding either	32.62% ±9.19%	25.81% ±8.58%	19.29% ±7.73%	10.51% ±6.01%
Attackers finding either	75.0% ±8.49%	69.23% ±9.05%	68.63% ±9.09%	45.19% ±9.75%

Table 3: Attack on different routing algorithms, attackers uses the Weighted Random Walk Insertion with length 4. Generated network has 100 nodes with 2 connections per node and 10% attackers.

Parameter	Algorithm 0:LND	Algorithm 1:RH len 4	Algorithm 2:RWI len 4
Singular possible sender/receiver sets	0.65%	1.17%	0.35%
Average number of hops	3.62	3.75	7.10
Average fee	1.05	1.19	3.41
Average possible sender size	12.13	11.15	10.87
Average possible receiver size	5.6	6.15	2.53
An attacker finding either	62.75% ±9.47%	62.57% ±9.49%	25.7% ±8.56%
Attackers finding either	82.18% ±7.50%	75.7% ±8.41%	59.22% ±9.63%

Table 4: Attack on Weighted Random Walk Insertion routing algorithm with different lengths, on snapshot of the Lightning Network with 0.4% attackers.

Parameter	length 4, g = 10	length 4, g = 4
Singular possible sender/receiver sets	4.26%	4.26%
Average number of hops	7.42	7.42
Average fee	15.38	15.38
Average possible sender size	1297.95	1297.95
Average possible receiver size	525.9	525.9
An attacker finding either	0.0%	0.0%
Attackers finding either	0.0%	0.0%

Table 5: Attack on Weighted Random Walk Insertion routing algorithm with different lengths. Generated network has 500 node network with a degree of 10, with different percentage of attacking nodes.

Parameter	2% lnd, g = 4	2% length 4, g = 4	10% length 4, g = 4
Singular possible sender/receiver sets	20.07%	0.0%	4.17%
Average number of hops	2.71	3.28	3.675
Average fee	0.59	0.94	1.11
Average possible sender size	97.47	100.87	1.94
Average possible receiver size	144.28	202.05	37.66
An attacker finding either	0.0%	0.0%	18.23% ±7.57%
Attackers finding either	0.0%	0.0%	23.33% ±8.29%

Conclusion

- The size and connectivity of the network is important for the anonymity of the transactions.
- There is a trade-off between anonymity and fee/hops.
- Random Walk Insertion algorithm improves the anonymity substantially from the simulations with snapshot, and the bigger generated network.
- For future research shadow routing could be tested, as it hides one of the essential information, time locks.
- More simulations with different percentages of attacker on the snapshot.

TU Delft
Delft University of Technology

References

[1] Kumble, Satwik Prabhu and Epema, Dick and Roos, Stefanie. (2021). How Lightning's Routing Diminishes its Anonymity. Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 1-10).
[2] Joseph Poon and Thaddeus Dryja. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. https://lightning.network/lightning-network-paper.pdf