Project Summary: Security and Privacy of Bitcoin's Lightning Network

1. Introduction
2. Lightning Network
    a. Routed payment network
    b. Payment channels
3. Vulnerabilities
    a. Lockdown
    b. Eclipse
    c. Probing

1. Introduction

Bitcoin is an emergent financial technology that stands in contrast to usual traditional payment networks like Visa and SWIFT by being open, decentralized, and allowing anonymous transactions. More than a financial product, Bitcoin is the implementation of a broader technology that allows distributed consensus and is known as blockchain. At the root of Bitcoin are 2 key technologies: the public ledger and the proof of work. The public ledger is a way for all participants in Bitcoin to monitor transactions and the set of UTXO. On the other hand, Bitcoin uses proof of work as its mechanism to validate transactions and have a unique view of the UTXO (see Byzantine Generals' problem). Minors serve this special role of confirming transactions and are compensated by receiving transaction fees and coinbase transactions -- incidentally geometrically increasing the Bitcoin money supply over time. As a result, a 1MB block is added every 10 minutes to the blockchain. This constrains the total amount of transaction possible and leads to low capacity and high transaction fees. How can we scale Bitcoin to solve these two problems? What are the risks entailed by scaling solutions?

2. Lightning Network

2.a Lightning Network, a routed payment network

Our project focuses on a technology that increases transaction capacity, reduces latency, and transaction fees at the same time by leveraging off-chain scaling. Off-chain scaling makes use of Bitcoin as a source of trust but outsources the high-volume transactional aspect to a satellite protocol. Lightning Network is a prominent off-chain solution anchored to Bitcoin that routes transactions through a network of channels held privately between users. As such, users create channels to one another when they connect to Lighting. If they want to transact with a user to whom they are connected with, they can transfer the correct amount in the trustless channel. Otherwise, they can create a route between unknown third parties that will eventually lead to the payee. This makes use of a combination of TOR and gossip protocols which will come under focus in the vulnerability section. Third parties are in turn incentivized to take part in the activity of Lightning by receiving a small transaction fee in the same way that Bitcoin does.

The major difference between Lightning and Bitcoin is that transactions are instantaneous and that there is no competition to have one's transaction feature on the uniquely shared blockchain, hence the lower fees.

2.b Lightning Payment Channels

At first blush, Lightning Network is nothing but a peer-to-peer routing network for transactions. But what makes Lightning work so well in practice is the trustless channel which has several desirable properties. First a lightning network gets created when two participants commit a shared amount on the blockchain. These funds serve as collateral and are used extensively in the Lightning protocol. Second, if Bob wishes to relay Alice's transaction to Carol, Bob's funds are never released to Carol before receiving the amount from Alice. This is made possible through HLTC. Besides the temporal sequencing of transactions, HTLCs cryptographically guarantee the identity of the payer and payee so that funds can't be lost in transit. The Lightning channels, hallmark of the off-chain solution, unlock astronomical speeds.

3. Vulnerabilities

Despite the various security features provided by Bitcoin, Lightning users still come under various threats due to intrinsic vulnerabilities in the Lightning Network.

3.a Lockdown attack

A lockdown attack takes advantage of the fact that HTLC locks the funds at a certain place as long as the whole route has not been established. Initially, this was used to avoid loss of funds when routing transactions. An attack can however flood a certain node with high amounts to virtually bankrupt the node for a limited period. This attack amounts to ephemeral denial of service and can be highly incapacitating. The problem stems from a cost of zero associated with creating transactions. A mitigation idea could be to impose a positive but small cost on attackers and users alike. Several caveats apply.

3.b Eclipse attack

Another threat is the eclipse attack. In this scenario an attacker poisons the network at large by creating several malicious nodes under his/her control. Again the cost of creating a node in the network is zero. Were the victim to connect exclusively to the attacker, the victim runs the risk of being taken advantage of up to losing one's balance.

3.c Probing attack

Finally, the probing attack is the focal point of our research. The attack leverages gossip protocol to receive information about the state of channels. This can lead to uncovering the actual amount normally hidden inside channels.

References

1. [n.d.]. https://github.com/ElementsProject/lightning.
2. [n.d.]. https://github.com/lightningd/plugins
3. [n.d.]. https://github.com/lightningd/plugins/tree/master/probe
4. [n.d.]. BOLT 7: P2P Node and Channel Discovery. https://github.com/ lightningnetwork/lightning-rfc/blob/master/07-routing-gossip.md
5. 2015. BIP 141. https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki.
6. 2019. SWIFT in figures. https://www.swift.com/sites/default/files/documents/ sif_201912.pdf.
7. A.M. Antonopoulos. 2014. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media. https://books.google.lu/books?id=IXmrBQAAQBAJ
8. Christian Decker and Roger Wattenhofer. 2015. A fast and scalable payment network with bitcoin duplex micropayment channels. In Symposium on Self- Stabilizing Systems. Springer, 3–18.
9. Yuhong Li, Kun Ouyang, Nanxuan Li, Rahim Rahmani, Haojun Yang, and Yiwei Pei. 2020. A blockchain-assisted intelligent transportation system promoting data services with privacy protection. Sensors 20, 9 (2020), 2483.
10. Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.