6.857 Network Security February 28th, 2017

6.857 Project Proposal: Bitcoin Lightning Network

Prof. Rivest, Kalal *Gina Yuan, Andrew Xia, Jamie Bloxham, Justine Jang*

1 Abstract

The Bitcoin Lightning Network is a research project currently ongoing at the Digital Currency Initiative as part of the MIT Media Lab. The Lightning network[2] is a set of nodes linked by 2-party payment channels built from Bitcoin smart contracts. The software is currently being built out and initially tested on the Bitcoin Testnet[1].

For this project, we wish to look for unknown or undocumented vulnerabilities in the software and specifications. Some previously mentioned potential vulnerabilities include novel cryptographic constructions, DoS-vulnerable communications, synchronization issues, key management, and database integrity issues. We may also look into side channel attacks and flaws in the user interface that may compromise the security of the system.

2 Plan

We are fortunate that this project is currently being undertaken by researchers here at MIT. In the coming weeks, we hope to meet with the researchers at the DCI to discuss how we may properly analyze the security of the Lightning system. We are searching for unknown vulnerabilities within the system, so it is likely that we may need to adopt an *ad hoc* strategy.

In the meantime, there are plenty of resources we can review to better understand the workings of the Lightning system, so that we will be prepared to tackle a comprehensive security analysis.

3 Glossary

- Payment channel: allows users to make multiple Bitcoin transactions without committing all of the transactions to the Bitcoin block chain
- Bitcoin smart contracts: Bitcoin uses a distributed contract to form agreements with people via the block chain.
- Bitcoin Testnet: an alternative Bitcoin block chain to be used for testing

References

[1] MIT Digital Currency Initiative, Lit, (2017), GitHub repository, https://github.com/mit-dci/lit

[2] Poon, J., Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Retrieved March 1, 2017, from https://lightning.network/lightning-network-paper.pdf.