Valerian Salh

CS 168

Dr. Thomas Austin

1 November 2021

Exploring Off-Chain Transactions

Bitcoin has strict limits on the size of blocks and transaction volume. Transaction volume is limited to 7 transactions per second on the network, while the size of a block is limited to 1 MB [1]. There are many arguments and some proposed solutions on how to address this issue, should Bitcoin grow significantly in terms of usage adoption. Currently, the main blockchain would be unable to service the transaction volumes that the current monetary and banking system manages on a regular basis. It is speculated that if Bitcoin was widely adopted for use, transactions would have to compete for recognition using fees [1], implying that the transaction fee cost of using the network would make the network impractical to operate on. One of the most notable solutions to Bitcoin's limits on transaction and block size is the Lightning Network, from which I will take inspiration and explore in my project.

The Lightning Network works by relying on Bitcoin and its native smart-contract scripting language [2]. An ordinary transaction that takes place on the base-layer of the Bitcoin network is known as an *on-chain* transaction. In contrast to this, the Lightning Network settles transactions *off-chain*. Note that this methodology is distinct from *sidechain* solutions, which work by transferring bitcoins to a separate blockchain (where transaction properties and rules may differ) to eventually be redeemed [1, 3].

I will give a brief explanation of the Lightning Network, with information gathered directly from its website [2]. The Lightning Network creates a bidirectional payment channel

between two willing participants on-chain, then allows these two participants to transact a seemingly limitless number of times off-chain, spending from the currently ledger entry output, until eventually the channel is closed and the final ledger entry is broadcasted to the Bitcoin network. The end result is that a single transaction will have been added to the blockchain, despite the two parties having transacted with each other numerous times. This entry on the blockchain can be closed at any time by either party. Many different bidirectional payment channels put together form the Lightning Network. As a result, two parties can transact with each other without having a direct payment channel between them. Instead, a path between some numbers of peer-to-peer intermediaries will be used to connect the two separate parties to allow them to transact with each other, similar to routing packets on the internet. Finally, in this scenario the blockchain acts as an arbiter that can enforce off-chain transactions once they come on-chain.

For my project, I will expand the UTXO implementation of SpartanGold to support off-chain transactions via a bidirectional payment channel that can be reused many times so long as the channel is open. Any time a transaction is made, both parties must sign an updated version of the inputs and outputs until finally, when a channel is closed, the latest transaction inputs and outputs are broadcasted to the network. If time permits and is feasible, I will also make an attempt to emulate the Lightning Network on a smaller scale by processing transactions between parties indirectly via a path of intermediaries.

References

[1] SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. https://jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf

[2] Lightning Network. https://lightning.network/

[3] Off-chain transactions. https://en.bitcoin.it/wiki/Off-chain_transactions

[4] Off-chain Transactions (Cryptocurrency). https://www.investopedia.com/terms/o/offchain-transactions-cryptocurrency.asp