Stroom: Liquid Deposits For Bitcoin Lightning Network

Abstract

Stroom DAO is a financial protocol between the Bitcoin Lightning Network and EVM-based blockchains (e.g. Ethereum). Stroom allows users to earn Lightning Network revenue without locking up BTC and maintaining their own node infrastructure. Users can deposit BTC into Stroom treasury and receive wrapped token lnBTC on EVM-based blockchains in return. The Stroom DAO stakes received liquidity into Lightning Networks channels where it earns yield via fees collected by Stroom's Lightning Network routing nodes. Stroom will launch in two phases. The first (bootstrapping) phase will allow the platform to be maintained by a closed set of Stroom's trusted Lightning Network node operators. The second (growth) phase will introduce decentralized governance, allowing the operation of a distributed set of Lightning Network nodes, picked by the Stroom DAO. The DAO members will control the protocol via BFT-style consensus, while node operators will manage, but not have access to users' funds deposited to Stroom.

Lightning Network Technology Overview

The Bitcoin network is the oldest, most widely recognized, and largest cryptocurrency by market capitalization. Bitcoin is inherently immutable through its decentralized protocol governance and is arguably the most secure cryptocurrency network. Bitcoin design emphasizes asset security, censorship resistance, and protection from abrupt total supply inflation. Together, these factors make Bitcoin better optimized as a digital store of value.

However, these features act as a tradeoff for others. For example, Bitcoin sacrifices performance to have very high security meaning it has limited transaction processing capacity. Limited processing capacity on the network means transaction costs can reach unreasonably high values, as happened in 2017-2018.

We have seen a large number of new blockchain technologies since the inception of Bitcoin in 2009, which have aimed to address the general problem of limited blockchain performance. It is clear that Bitcoin's scalability problem couldn't be solved on Bitcoin's protocol level. Many projects came into existence that proposed 'layer-2' scalability problem solutions: sidechains, wrapping Bitcoins on more scalable chains (e.g., Ethereum, Solana, etc), and Lightning Network (LN) [3].

The key distinction of the LN from other scaling solutions is its security model. Sidechains effectively are other blockchains with their own security guarantees, which usually are much less attractive than those of Bitcoin. Hence, there are higher chances to lose BTC, if those BTC are stored on sidechains or any other blockchain.

In contrast, Lightning Network does not utilize any chain at all, except the native Bitcoin chain.

Payments are routed through the distributed network of payment channels - 2-of-2 multisig outputs, which are created and settled on the Bitcoin blockchain. This is how the scalability effect is achieved - big numbers of LN transactions are processed in a single channel, which requires only two on-chain transactions to operate. In general, a channel is closed only when one or both participants decide not to run that channel, or in dispute situations.

From the other perspective, Lightning Network is a network of nodes that are connected with each other by payment channels. Any node can find a path to any other node and securely route the payment along that path. The process is somewhat similar to how data packages are routed on the Internet. Since LN directly sends the value, a small fee can be efficiently subtracted from each payment in favor of intermediary nodes. Moreover, it is very natural to reward routing nodes in that way, since they are providing BTC liquidity in channels, crucial for the security of the whole transaction. This opens up an opportunity for a new business - routing payments in LN.

Recently, several individuals claimed that they managed to set up a profitable LN node, that is profiting solely on routing LN payments [11]. However, hosting and managing a routing LN node is not practical for tech-unsavvy users at this moment because of the technical complexities of running their own routing hub.

The more BTC value stacked in channels in the network, the more payments can be routed. Therefore attracting more liquidity to Lightning Network positively influences the whole Bitcoin ecosystem.

Reducing technical barriers for nodes and users is critical for the long-term success of LN. Users extract exponentially more value from the LN with a growing set of nodes and interconnected channels as it makes it more likely for that user to transact with a target vendor.

The LN has seen promising growth since 2021 with over 5000 BTC deposited across 17,000+ nodes operating 80,000 channels. Representing less than 0.02% of the circulating BTC supply, LN has yet to reach mainstream adoption.

Introducing Stroom

Stroom aims to provide the bridge between the LN and DeFi ecosystems across all EVM-compatible chains, beginning with Ethereum. Stroom reduces the technical burden associated with depositing Bitcoin into the LN while simultaneously enabling users to yield-farm in EVM-compatible DeFi ecosystems. The Taro protocol [14] also enables other assets (e.g. stablecoins) to be deposited into LN positioning Stroom as a multi-asset yield product for Lightning Network.

The primary goals of Stroom are:

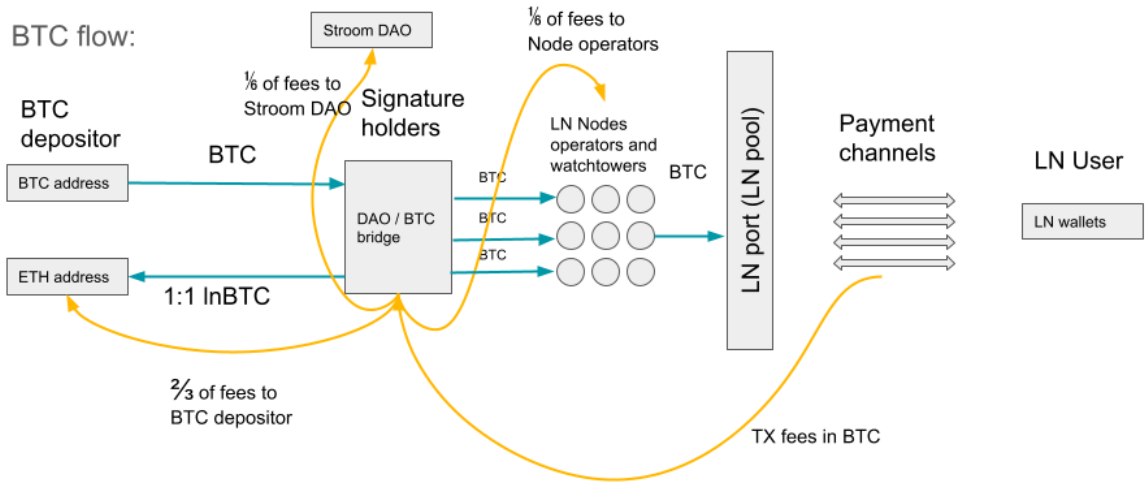
- To allow users to generate returns by depositing their Bitcoin to the LN and DeFi simultaneously
- To remove the technical burden of self-hosting a routing node
- To contribute to Bitcoin's scalability by enhancing the capacity of the LN
- To provide lnBTC (a wrapped BTC token as a building block for the DeFi ecosystem)

In phase 1, Stroom will operate with a centralized set of LN node operators before transitioning to a DAO-governed decentralized architecture in phase 2.

Protocol Architecture

In order to use Stroom, a user is just required to deposit his Bitcoins into the project's treasury, which will automatically send back lnBTC on an Ethereum chain. The deposit of Bitcoins into LN channels and user rewards distribution will be processed automatically by the Stroom DAO. To make it possible we introduce three main components of the project:

- ***Bridge with Ethereum:*** Stroom will start with an Ethereum integration because this is the most popular DeFi chain at the moment of writing this paper. More chains will be added later.
- **Stroom-enabled LN nodes or hubs**
- **Stroom ledger (required for proper DAO operations)**



Stroom Bridge

When a user sends BTC to Stroom it is credited to the Stroom DAO treasury. Simultaneously, the corresponding amount of lnBTC, an ERC-20 token, is minted on Ethereum through a bridging process. This lnBTC is composable with the broader DeFi ecosystem on Ethereum, similar to other Ethereum assets such as Lido [12] Finance's stETH

The treasury and bridge are based on a K-of-N multisig federation where each member of the federation monitors both ETH and BTC blockchains. For each lnBTC minting, redemption, or LN channel opening and closing, the operation is approved by the K-of-N signature holders. Dividends from LN will be distributed in the form of lnBTC.

In order to keep the 1:1 peg of lnBTC to BTC, Stroom will enable users to redeem their lnBTC directly for BTC. Some portion of BTC liquidity staked in the protocol is kept idle in Stroom's BTC treasury where these reserves are used for processing redeem transactions. Small redemption fees will be deducted from the balance in order to compensate for related transaction costs.

Stroom-Enabled Lightning Network Hubs

Routing LN nodes that are part of the system must be compliant with both the Stroom protocol and the Stroom ledger. They will not have access to the BTC stored in their channels and every operation updating channel state will be authorized by federation signature holders.

The hub's channel side will be managed with a K-of-N federation multi-signature script as opposed to a single private key as in a classical LN. This will be achieved by utilizing Taproot-compatible LN channels [7].

In addition to private key delegation to the federation, it is also required that nodes post all revoked channel states signed by the channel counterparty to the Stroom ledger. Therefore, the Stroom-enabled hub serves as a connection proxy to the federated lnd, managed by the federation. This creates a Stroom Watchtower [5], monitoring the channel's state. If an LN node does not cooperate with the rules established by the federation, the federation will remove that LN from the system by closing all of its channels.

Stroom Ledger

Federation signature holders will communicate with each other through the Stroom ledger, where they and Stroom-enabled LN hubs can exchange, store and produce necessary operational data.

Such processes include storing current channel states and revocation keys and updating LN state signatures. For example, all minting and redemption multi-party signatures will be formed

using the Stroom ledger, where LN-enabled hubs can immediately access them.

Stroom ledger is a simple pBFT-style consensus blockchain. Each federation signature holder will run a full Stroom validating node in order to enforce censorship resistance. Aiming to support bridging, each full node will also have integrated Bitcoin and Ethereum full nodes. Full nodes will collectively serve as a DAO-run LN watchtower since federation signature holders are able to monitor LN channels through Bitcoin nodes. All required revocation keys will be stored on the ledger.

Stroom DAO Structure

The Stroom protocol operates on top of three protocols that are constantly evolving: Bitcoin, Ethereum, and the Lightning Network. In order to operate securely and in a trustless manner, it is necessary for Stroom to leverage reliable communication between those protocols.

There are many Bitcoin-Ethereum bridges that are secure and trustless, which already are organized as multisig DAOs, e.g. RenBTC, others are secure but not necessarily fully trustless (e.g. wBTC) with several organized as multisig vaults among centralized custodians.

In order to stake liquidity in LN channels in a trustless manner, there should be a multi-party signature computation mechanism that will govern user funds. Distributed governance through a DAO structure can greatly increase transparency and will provide community input in decision-making processes. The community will be able to:

- Establish and modify incentives for signature holders to behave honestly
- Replace a signature holder (if required)
- Upgrade the Stroom protocol by proposing and adopting changes in underlying protocols
- Fund the development of the protocol and core functionality from the DAO treasury
- Govern funds from collected service fees

Tokenomics

There will be two tokens associated with the protocol: lnBTC and STROOM. lnBTC is LN-staked Bitcoin wrapped in the Ethereum blockchain while STROOM is the DAO governance token.

lnBTC

lnBTC is an ERC-20 token that can be redeemed 1:1 for BTC. lnBTC is a liquid derivative of BTC staked in Lightning Network. We plan on integrating lnBTC into blue-chip DeFi protocols across the ecosystem, much as stETH has been integrated across various protocols.

BTC that is deposited during the minting of lnBTC will be deposited into LN channels by

Stroom-enabled LN hubs to generate rewards. Hub balances are monitored and their returns are redistributed to lnBTC holders daily, similar to how Lido [12] distributes rewards, subject to service fees.

The minimum BTC deposit to the Stroom protocol will initially be 0.01 BTC. Minting lnBTC is subject to approval by the federation of signature holders. When lnBTC is redeemed by a user, the redemption of BTC to the user's Bitcoin address is also approved by the federation of signature holders.

STROOM

STROOM is Stroom's native cryptoasset and provides holders voting power on DAO proposals regarding key network parameters. Vote weights for DAO participants are proportional to how many STROOM tokens a user stakes in the voting contract.

Another role of the governance token is its utility within the staking mechanism. Federation signature holders will be required to stake the DAO tokens as collateral, to ensure that those crucial ecosystem participants have "skin in the game". Exact slashing mechanics for signature holders can be upgraded by DAO proposals.

Stakeholder Incentives

There are three primary stakeholders within the Stroom protocol: protocol users, node operators, and DAO signature holders.

Protocol users are incentivized to deposit BTC financially by two main yield streams: yield generated by LN routing fees and DeFi ecosystem participation with the lnBTC derivative. Node operators who are responsible for managing LN nodes are incentivized to carry out their operations with a 15% share of LN yield proceeds, which can be changed through governance processes. Federation signature holders are also incentivized to run the project by STROOM supply issuance and 15% of the routing fees collected on LN.

Risks

Smart Contracts Security Risks. Bugs in smart contracts have the potential to lead to loss of funds. While it is impossible to fully eliminate such risks, we devote substantial resources to mitigate them. Stroom will partner with specialized companies to perform security audits as well as establish a bug bounty program.

LN Software Security Risks. The LN and associated technology is still experimental and rapidly evolving. Since our project relies heavily on LN software developed by the community, it is possible that LN native bugs could lead to the loss of Stroom-associated funds. We minimize

those risks by choosing one of the most developed, tested, and adopted realizations of the LN daemon - lnd [4].

LN Slashing Risk. The LN protocol employs a disincentive mechanism for LN nodes, that slashes the stakes of broadcasting channels closing transactions with the wrong state. It is possible that an LN node could accidentally broadcast such a transaction. To mitigate this risk, we use the DAO approval mechanism for the channel closure procedure. It is also possible that an LN node operator could miss the chance to prevent a slashing event due to several factors (e.g. simply overlooking the fraudulent transaction or Bitcoin blockchain congestion). We integrate a DAO-run watchtower to mitigate such risks.

LN Adoption Risk. In the case of low LN protocol adoption as a payments rail, the value proposition of the Stroom protocol for users is diminished. LN adoption greatly depends on the amount of liquidity present in LN.

DAO Threshold Signature Risks. The DAO approval mechanism is subject to risk. Federation signature holders can be compromised, or could even collude to attack the protocol. To prevent that, we chose only trusted and professional federation signature holders and ensure that they have a slashable stake in the protocol as collateral.

lnBTC Price Risk. There is a risk that lnBTC will lose its peg to BTC. In order to prevent that, we have designed a smooth and secure minting and redemption process. Users will always have the opportunity to swap lnBTC for BTC at a 1:1 ratio forming an arbitrage for market participants. This will be subject to the fund's availability in the treasury and the Stroom DAO will need to ensure a sufficient number of LN channels can close to facilitate the redemptions in full.

Conclusion and Future Directions

Stroom aims to leverage recent technological advances in the Bitcoin ecosystem to provide a new path to accessing Bitcoin yield while enhancing BTC's bridge to alternative DeFi ecosystems. Increasing the LN capacity will contribute to the adoption of Bitcoin technology as a rail for payment solutions and drive higher potential yields for LN depositors - thereby creating a positive feedback loop.

There are several directions for future research to advance Stroom. We are planning to adopt the Eltoo [8] scheme for payment channels, which is currently blocked due to the adoption of BIP-118 [9]. This will diminish the computational overhead for federation signature holders.

DAO governance is the most experimental and fast-developing area in the crypto field. We will dedicate a portion of our research resources to ensure we develop a robust DAO governance structure, and leverage existing partnerships. Stroom could also incorporate native Bitcoin smart contracts based on BIP-119 [10] opcode CHECKTEMPLATEVERIFY to further decentralize our protocol and enhance its security.

References:

[1]: The Block. Assets in Defi
https://www.theblockcrypto.com/data/decentralized-finance/asset-management

[2]: Bitcoin Visuals. Lightning Network Capacity
https://bitcoinvisuals.com/ln-capacity

[3]: Lightning Network Whitepaper
https://lightning.network/lightning-network-paper.pdf

[4]: Lightning Labs. lnd
https://github.com/lightningnetwork/lnd

[5]: Watchtower in Lightning Network
https://github.com/lightningnetwork/lnd/blob/master/docs/watchtower.md

[6]: Lightning Network Devs mailing list. PTLC.
https://lists.linuxfoundation.org/pipermail/lightning-dev/2021-October/003278.html

[7]: Lightning Network Devs mailing list. Taproot.
https://lists.linuxfoundation.org/pipermail/lightning-dev/2019-December/002375.html

[8]: ELTOO
https://blockstream.com/eltoo.pdf

[9]: Bitcoin Improvement Proposals. SIGHASH_ANYPREVOU
https://github.com/bitcoin/bips/blob/master/bip-0118.mediawiki

[10]: Bitcoin Improvement Proposals. CHECKTEMPLATEVERIFY
https://github.com/bitcoin/bips/blob/master/bip-0119.mediawiki

[11]: Nasdaq. Running profitable Lightning Network Node
https://www.nasdaq.com/articles/four-tips-for-running-a-profitable-lightning-network-node-2021-07-22

[12]: Lido Whitepaper
https://lido.fi/static/Lido:Ethereum-Liquid-Staking.pdf

[13]: Lightning Pool
https://lightning.engineering/pool/

[14]: Taro Protocol
https://docs.lightning.engineering/the-lightning-network/taro