Stroom: Liquid Staking Derivative Protocol For Bitcoin Lightning Network

Viacheslav Zhygulin s@stroom.network, Rostyslav Shvets r@stroom.network v.0.4

Abstract

Stroom DAO is a liquid staking derivative protocol for the Bitcoin Lightning Network operating on EVM-based blockchains like Ethereum. By utilizing Stroom, users have the opportunity to earn revenue from the Lightning Network without the need to lock up their BTC or maintain their own node infrastructure. To participate, users can deposit their BTC into the Stroom treasury and, in return, receive wrapped tokens called stBTC and bstBTC on EVM-based blockchains. The Stroom DAO then utilizes the staked liquidity to engage in Lightning Network channels, where it generates yield through the fees collected by Stroom's Lightning Network routing nodes. The launch of Stroom will occur in two phases. The initial phase, known as the "bootstrapping" phase, will involve a closed group of trusted Lightning Network node operators but a diverse group of validating nodes maintaining the bridging platform chosen by the DAO governance process. In the subsequent "growth" phase, DAO governance will enable a distributed network of Lightning Network nodes set up trustlessly but still chosen by the Stroom DAO through a specialized KYC process. In that sense, protocol control and development will always be governed by DAO members through DAO voting, validating members will approve operations with treasury through a BFT-style consensus, and Lightning Network nodes will be responsible for managing channels' liquidity without direct access to its funds.

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. 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 for 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 many 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 are much less attractive than those of Bitcoin. Hence, there are higher chances of losing 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 created and settled on the Bitcoin blockchain. This is how the scalability effect is achieved - enormous numbers of LN transactions are processed in a single channel, requiring only two on-chain transactions. Generally, 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 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, which is crucial for the security of the whole transaction. This opens up an opportunity for a new business - routing payments in LN.
Some individuals have recently asserted that they have successfully established a profitable Lightning Network (LN) node solely focused on routing LN payments [11]. However, due to the current technical intricacies involved in setting up and managing a routing LN node, it is impractical for users without strong technical skills to engage in such endeavors.

Moreover, a higher liquidity level within the Lightning Network directly correlates with an increased throughput capacity. As more BTC value is stacked in the channels of the network, a greater number of payments can be efficiently routed. This improved throughput not only enhances the efficiency and speed of transactions within the Lightning Network but also positively impacts the overall Bitcoin ecosystem. By attracting additional liquidity to the Lightning Network, the entire ecosystem benefits from enhanced scalability and the ability to handle a greater volume of transactions.

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, making it more likely for that user to transact with a target vendor successfully.

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

Introducing Stroom

Stroom's objective is to establish a connection between the Lightning Network (LN) and the decentralized finance (DeFi) ecosystems on various EVM-compatible chains, starting with Ethereum. By doing so, Stroom alleviates the technical complexities involved in depositing Bitcoin into the LN while concurrently providing users with the opportunity to participate in yield farming within EVM-compatible DeFi ecosystems. Additionally, the Taproot Asset protocol [14] facilitates the deposit of other assets, such as stablecoins, into the LN, positioning Stroom as a versatile yield product that supports multiple assets within the Lightning Network.

The primary goals of Stroom are:

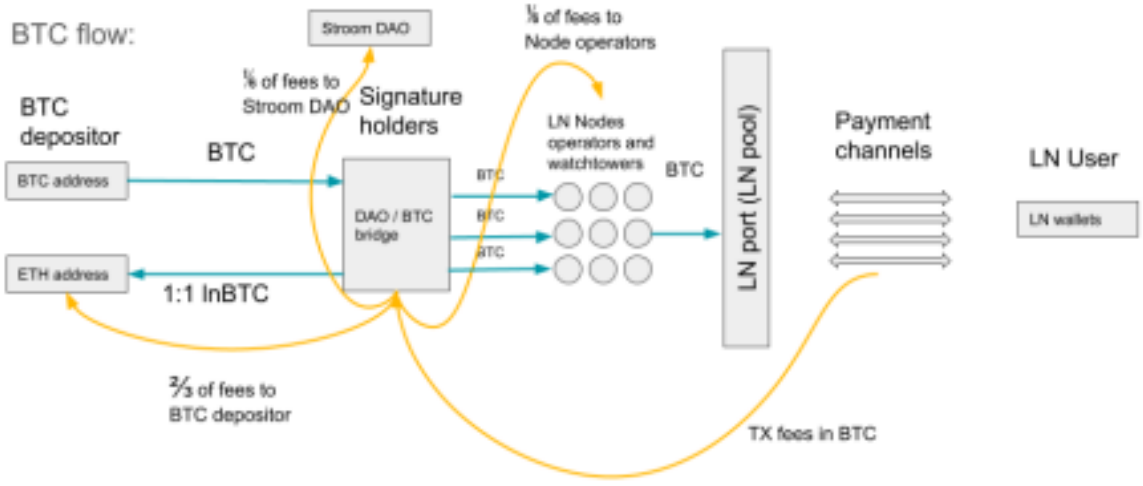
- To allow users to generate returns by depositing their Bitcoin to the LN and DeFi simultaneously
- To remove the technical burden of self-hosting a routing LN node
- To contribute to Bitcoin’s scalability by enhancing the capacity of the LN
- To provide stBTC and bstBTC(wrapped BTC tokens) as a building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

During the initial phase, known as Phase 1, Stroom will function with a centralized group of Lightning Network (LN) node operators; however, it will incorporate a decentralized BTC-ETH Bridge. Subsequently, in Phase 2, Stroom will undergo a transition towards a decentralized autonomous organization (DAO)-governed LN node management approach.

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 Stroom DAO handles the automatic processing of Bitcoin deposits into LN channels and the distribution of user rewards. To enable this functionality, the project introduces three primary components:

- ***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 validating nodes,** which are required for proper DAO operations



Stroom Bridge

When a user sends BTC to Stroom, it is credited to the Stroom DAO treasury. Simultaneously, users are provided with the option of minting the corresponding amount of either stBTC or

bstBTC on Ethereum through a bridging process. These stBTC and bstBT tokens are 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. The K-of-N validating nodes approve the operation for each lnBTC minting, redemption, or LN channel opening and closing. Dividends from LN routing 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 stBTCdirectly 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

All routing LN nodes within the system must adhere to the Stroom protocol and comply with its requirements. These nodes will not possess access to the BTC held within their respective channels, and any action that modifies the channel's state will require authorization from validating nodes.

To manage the channel side of the hub, a K-of-N federation multi-signature script will be employed instead of relying on a single private key, as is typically done in traditional LN setups. This implementation will be accomplished by utilizing Taproot-compatible LN channels [7] with Schnorr threshold signatures.

In addition to delegating private keys to the federation, it is mandatory for LN nodes to submit all revoked channel states, signed by the corresponding channel counterparty, to the databases of Stroom validating nodes. Consequently, the Stroom-enabled hub acts as a connection proxy to the federated Lightning Network Node, run by validating nodes. This configuration establishes an inherent Stroom Watchtower [5] functionality that automatically monitors the state of the channels. If an LN node fails to comply with the rules established by the federation, the

federation will take action by closing all channels associated with that non-compliant LN node and removing it from the system.

Stroom Validating Nodes Consensus

The FROST algorithm, a Schnorr threshold signing algorithm, will be utilized by validating nodes to generate approvals for various operations. However, it is important to note that each validating node independently validates each event that requires approval without relying on other nodes. To finalize an approval, a minimum of 2/3 + 1 votes from the validating nodes is required.

Stroom processes involve storing current channel states and revocation keys, as well as updating LN state signatures. For instance, all multi-party signatures for minting and redemption will be generated and stored in the validating nodes' local database, which LN-enabled hubs can promptly access.
Their local databases can synchronize similarly to a pBFT-style consensus blockchain, where each Stroom validating node can access each other Stroom validating nodes to ensure censorship resistance. To support bridging, each full node will also integrate Bitcoin and Ethereum full nodes. These full nodes will collectively serve as a DAO-managed LN watchtower, as validating full nodes can monitor LN channels through Bitcoin nodes. The necessary revocation keys will be stored within the local databases.

Stroom DAO Structure

The Stroom protocol operates on top of three constantly evolving protocols: 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 significantly 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 validating node (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 three tokens associated with the protocol: stBTC, bstBTC, and STROOM. stBTC and bstBTC are LN-staked Bitcoin wrapped in the Ethereum blockchain, while STROOM is the DAO governance token.

stBTC and bstBTC

stBTC and bstBTC are liquid derivatives of BTC staked in Lightning Network. We plan on integrating stBTC and bstBTC into blue-chip DeFi protocols across the ecosystem, much as stETH has been integrated across various protocols. However, it's specifically bstBTC that provides the unique opportunity for users to earn a yield in native Bitcoin, while also offering the freedom to convert their bstBTC back to BTC at any moment.

BTC that is deposited during the minting of stBTC or bstBTC will be deposited into LN channels by Stroom-enabled LN hubs to generate rewards. Hub balances are monitored, and their revenues are redistributed to the token holders daily, similar to how Lido [12] distributes rewards, subject to service fees.

Initially, the Stroom protocol will require a minimum BTC deposit of 0.01 BTC. The minting of stBTC and bstBTCis contingent upon approval from the federation of validating nodes. Similarly, when a user seeks to redeem bstBTC, the redemption of BTC to the user's Bitcoin address must also receive approval from the federation of validating nodes. When executed correctly, these operations should be seamlessly processed by the validating nodes, as this behavior is ingrained within the Stroom protocol.

STROOM

STROOM serves as the native cryptocurrency of Stroom, granting holders voting power in DAO proposals that determine important network parameters. The voting influence of DAO participants is proportionate to the number of STROOM tokens they stake within the voting contract.

Additionally, the governance token plays a vital role in the staking mechanism. Both validating nodes and Stroom-enabled hubs are required to stake DAO tokens as collateral to ensure active participation and a vested interest in the ecosystem. The specific mechanics for penalizing or slashing these tokens can be improved through DAO proposals, allowing for upgrades to the slashing mechanisms for validating nodes and Stroom-enabled routing hubs.

Stakeholder Incentives

The Stroom protocol involves three key stakeholders: protocol users, LN node operators, and validating nodes.
Protocol users are motivated to deposit BTC due to two primary sources of financial yield: earnings of 65% from LN routing fees and participation in the DeFi ecosystem through the derivative tokens.

Node operators, who handle the management of LN nodes, are incentivized by receiving a 15% share of the LN yield generated by his/her node. It's important to note that this percentage can be modified through governance procedures.

Federation signature holders are also encouraged to actively participate in the project, receiving 10% of the routing fees collected on the LN network.

A portion of the revenue, specifically 10%, is allocated to the DAO treasury as a stabilizing fund. Additionally, this amount may be distributed to long-term STROOM token holders as an incentive.

Upon the project's launch, different programs for STROOM token issuance incentivization will be implemented. The specific programs will be determined based on an analysis to identify which category of users requires incentivization.

Risks

Smart Contracts Security Risks: The presence of bugs in smart contracts poses a potential threat to fund loss. While it is impossible to entirely eliminate these risks, we allocate significant resources to mitigate them. Stroom will collaborate with specialized companies to conduct security audits and establish a bug bounty program.

LN Software Security Risks: The LN technology and its associated software are still experimental and rapidly evolving. As our project heavily relies on LN software developed by the community, there is a possibility that native LN bugs could result in the loss of Stroom-associated funds. To minimize these risks, we have chosen one of the most developed, tested, and widely adopted LN daemon implementations - lnd [4].

LN Slashing Risk: The LN protocol incorporates a disincentive mechanism for LN nodes, which slashes the stakes of nodes that broadcast channel closure transactions with incorrect states. There is a potential for accidental broadcasting of such transactions by an LN node. To mitigate this risk, we employ the DAO approval mechanism for the channel closure process. Additionally, there is a possibility that an LN node operator may overlook a fraudulent transaction or face Bitcoin blockchain congestion, resulting in a missed opportunity to prevent a slashing event. To address this, we integrate a DAO-run watchtower to mitigate such risks.

LN Adoption Risk: If the adoption of the LN protocol as a payment rail remains low, the value proposition of the Stroom protocol for users may be diminished. The adoption of LN relies heavily on the presence of sufficient liquidity within the network. Moreover, introduction of stablecoins to LN through Taro Asset Protocol will greatly boost LN adoption.

Validating Nodes Threshold Signature Risks: The DAO approval mechanism is exposed to certain risks. Federation validating nodes may be compromised or collude to attack the protocol. To prevent this, we carefully select trusted and professional validators, ensuring that they hold a slashable stake in the protocol as collateral.

stBTC/bstBTC Price Risk: There is a risk tha derivative tokens may deviate from its peg to BTC. To mitigate this, we have designed a secure and seamless minting and redemption process. Users will always have the option to swap stBTC for BTC at a 1:1 ratio, which creates arbitrage opportunities for market participants. However, the availability of funds in the treasury and the Stroom DAO's ability to facilitate sufficient channel closures will be crucial in facilitating

full redemptions. Still, in the worst case of a bank run situation, Stroom can close a significant portion of channels in order to process redemptions.

Conclusion and Future Directions

Stroom aims to capitalize on recent technological advancements in the Bitcoin ecosystem, offering a new avenue for accessing Bitcoin yield while strengthening BTC's connection to alternative DeFi ecosystems. By increasing the LN capacity, the adoption of Bitcoin technology as a payment solution will be fostered, resulting in higher potential yields for LN depositors. This, in turn, creates a positive feedback loop.
In terms of future research directions, Stroom plans to embrace the Eltoo scheme [8] for payment channels, which is currently hindered by the adoption of BIP-118 [9]. This implementation will reduce the computational overhead for federation signature holders, improving efficiency. Additionally, Stroom may integrate native Bitcoin smart contracts based on BIP-119 [10] opcode CHECKTEMPLATEVERIFY, further decentralizing the protocol and enhancing its security.

DAO governance represents an experimental and rapidly evolving area in the crypto field. To ensure a robust DAO governance structure, we will allocate research resources and leverage existing and most recent developments in this field.

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-2021-0 7-22

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

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

[14]: Taproot Asset Protocol
https://docs.lightning.engineering/the-lightning-network/taproot-assets

[15]: FROST algorithm
https://eprint.iacr.org/2020/852.pdf