Super Bitcoin

A Value Internet Sharing Bitcoin’s Consensus Security

Author: BEVM, October 2024

Abstract

Super Bitcoin is a value-based internet centered around BTC, and sharing Bitcoin's consensus security. This value internet not only inherits the security of the existing Bitcoin network but also transcends BTC's current limitations of being solely used for transfer, providing the Bitcoin network with unlimited scalability and flexibility.

Although the Lightning Network [2] inherits Bitcoin's network security and offers partial scalability solutions, it still falls short in supporting smart contracts and further enhancing scalability. We propose a five-layer architecture for Super Bitcoin using the Bitcoin network as the kernel layer, maintaining system security and transaction irreversibility through the proof-of-work (PoW) consensus mechanism; building an efficient communication layer based on the Lightning Network, facilitating rapid transmission of asset information while preserving Bitcoin's decentralized nature; we introduce the Taproot Consensus as the extension layer, abstracting Lightning Network communication and asset information to provide a standardized interface for the upper virtual machine layer; a multi-chain layer, also known as the fusion layer, consists of multiple lightning chains secured by BTC consensus, integrating any mainstream virtual machine (VM) to achieve a "Multi-chain interconnection“ and ”multi-chain interoperability” unified by BTC consensus; finally, at the application layer, providing developers with rich tools and interfaces to build a decentralized application (DApp) ecosystem, all sharing the security of BTC consensus.

1. Introduction

As the pioneer of cryptocurrencies, Bitcoin (BTC), through its proof-of-work (PoW) consensus mechanism and decentralized network structure, has garnered an immense level of consensus, becoming a supranational currency. This security stems from the perfect combination of its vast network hash power and economic incentives. The birth of Bitcoin not only ushered in a new era of decentralized digital currency but also pointed the way for the subsequent development of blockchain technology. However, the limitations of Bitcoin’s scripting language soon became apparent, as it only supports simple value transfers and limited contract logic, unable to meet the demands of more complex decentralized applications.

The evolution of blockchain technology is essentially all about expanding and enhancing Bitcoin's capabilities. Vitalik Buterin, the founder of Ethereum, initially envisioned adding

smart contract functionality to Bitcoin. However, due to the technological constraints of the time and the limitations of the Bitcoin network, Ethereum had to establish its own independent consensus system. While this approach allowed for the creation of Turing-complete smart contracts, it also introduced new security risks and scalability challenges. Many projects followed suit, building independent blockchain ecosystems, gradually diverging from and even forgetting the original intention of extending Bitcoin's capabilities.

However, two key factors remind us of the need to reconsider this direction. First, the continued rise in Bitcoin's value relative to other cryptocurrencies like Ethereum has validated the trust people place in its security and stability. Second, the collapse of Luna/UST, which wiped out nearly $100 billion in market value, highlighted the severe security vulnerabilities present in independent consensus chains, especially when faced with complex economic models and rapidly growing network value.

In this context, we introduce Super Bitcoin to create a true value internet sharing Bitcoin's consensus security. It fundamentally differs from the existing Bitcoin Layer 2 solutions: traditional Bitcoin Layer 2 solutions (such as the Lightning Network) mainly achieve fast payments through off-chain state channels and limited scripts, while sharing Bitcoin's consensus security but lacking flexibility. Meanwhile, sidechains like Stacks or Layer 2 solutions, although they support smart contracts, still rely on independent multi-signature mechanisms for security, thus not fully inheriting the security of the Bitcoin mainnet.

2. Technical Background

To fully understand the proposed solution, it is necessary to first review the background and development of several key technologies. This chapter briefly introduces the Lightning Network, the Substrate framework [3], BEVM's Taproot Consensus, and the multi-chain interoperability system to provide a foundation for understanding our solution.

2.1 Lightning Network

The Lightning Network is a Layer2 scaling solution for Bitcoin, with its core design principles detailed in the BOLT (Basis of Lightning Technology) specifications. These specifications not only ensure the efficient operation of the Lightning Network but also ingeniously achieve deep integration with the consensus security of the Bitcoin mainnet. Several parts of the BOLT specifications play a key role in sharing Bitcoin's consensus security.

BOLT #2 and BOLT #3 provide detailed guidelines on the lifecycle management of payment channels and the structure of transactions. The opening of a channel involves creating a multi-signature output on the Bitcoin blockchain, while closing the channel requires broadcasting the final state to the mainnet. BOLT #3 specifically defines commitment transactions, which are the core mechanism by which the Lightning Network shares Bitcoin's consensus security. Each time the channel state is updated, a new commitment transaction is generated, which can be broadcast to the Bitcoin mainnet if needed. The design of commitment transactions ensures that even if one party in the channel becomes

uncooperative, the other party can still close the channel by broadcasting the most recent commitment transaction and receive their due funds. This mechanism directly relies on Bitcoin’s consensus rules and security, meaning the Lightning Network’s security is essentially guaranteed by the Bitcoin network.

BOLT #5 defines the penalty mechanism for channel closures. This mechanism introduces the concept of "revocating private keys," effectively preventing participants from broadcasting outdated channel states. If dishonest behavior is detected, the honest party can use these keys to punish the other party on the Bitcoin main chain, thereby ensuring the accuracy of the channel state and enforcing honest behavior among participants through Bitcoin's consensus mechanism.

Additionally, the commitment transaction format specified in BOLT #3 connects Lightning Network transactions to Bitcoin's fee market through "anchor outputs." This not only enhances the security of transactions but also ensures that Lightning Network transactions can still be confirmed promptly during periods of network congestion.

These meticulously designed specifications collectively ensure that the Lightning Network, while providing fast and low-cost transactions, can still fully leverage Bitcoin's robust consensus security.

2.2 Substrate Framework

The Substrate framework is a highly modular blockchain development toolkit written in Rust, providing a powerful and flexible technical foundation for the implementation of Super Bitcoin. Its core strength lies in its pluggable Pallet system, where these pre-built functional modules serve as "blockchain Legos," enabling us to quickly and efficiently assemble and customize the desired features.

For Super Bitcoin, Substrate's modular design is crucial. It allows us to flexibly build and integrate various functional components on top of the shared Bitcoin consensus security. By leveraging Substrate's Pallet, we can easily support and integrate different virtual machine environments, thereby increasing the system's flexibility and adaptability. This design not only accelerates the development process but also provides Super Bitcoin with powerful scalability, allowing it to better meet the evolving needs of the blockchain ecosystem.

Super Bitcoin utilizes these features of Substrate to customize the **BEVM-stack framework**, which enables one-click deployment of lightning chains.

2.3 Taproot Consensus

BEVM’s Taproot Consensus integrates Bitcoin’s Taproot upgrade [4] technology. This technology combines several key elements: Schnorr signatures [5] provide signature aggregation capabilities, Merkelized Abstract Syntax Tree (MAST) support complex conditional scripts, and Musig2 enables two-round communication in multi-signature schemes. Through the combination of these technologies, BEVM successfully implements a decentralized threshold signature network with (t, n) support.

Additionally, BEVM leverages Bitcoin SPV (Simplified Payment Verification) technology to achieve lightweight decentralized block header synchronization. This allows transaction verification without downloading the full blockchain data, enabling BEVM to synchronize with the BTC mainnet in a decentralized manner. In Super Bitcoin architecture, Taproot Consensus plays a key role as the extension layer: it interfaces with the Lightning Network below, abstracting and integrating asset information, and provides standardized interfaces for different virtual machine execution environments above, realizing the transmission and utilization of asset information.

Such design makes Taproot Consensus a core component of the Super Bitcoin architecture. It not only inherits the security and privacy-preserving characteristics of the Bitcoin network but also provides rich functional support for upper-layer applications.

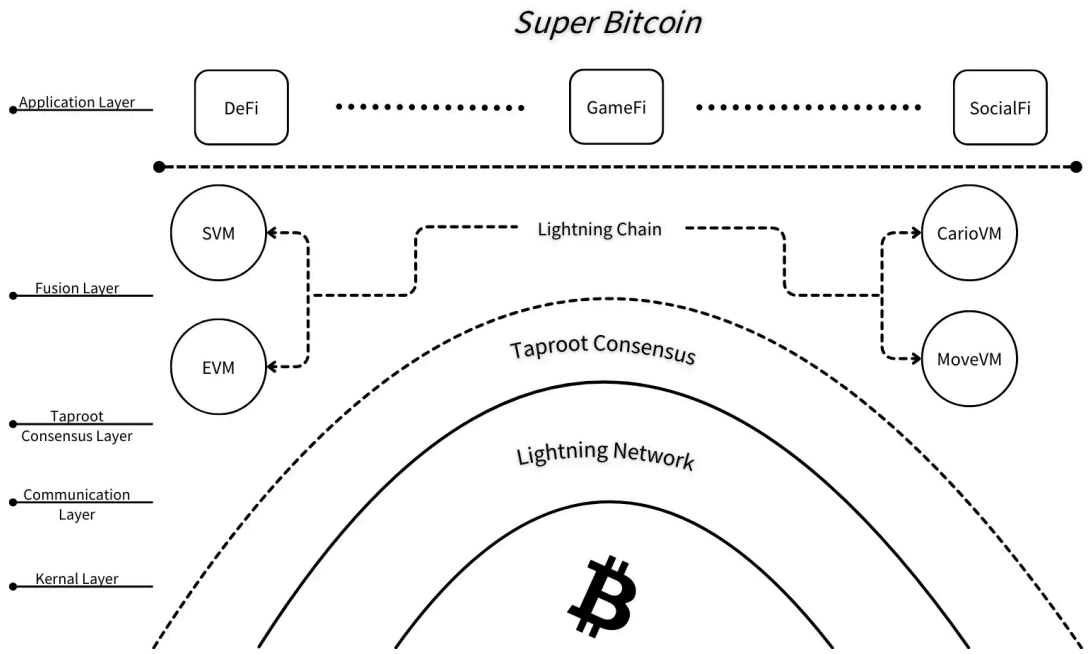
2.4 Multi-Chain Interoperability System

The concept of a multi-chain interoperability system was first introduced by Polkadot. Polkadot [6] is a multi-chain interoperability system based on the Substrate framework, sharing the security of DOT consensus, and using parachains for application chain expansion. Correspondingly, **Super Bitcoin** is a multi-chain interoperability system built on Bitcoin and the Lightning Network, sharing BTC consensus security, and using Lightning Chains for application chain expansion.

The differences between the two are as follows:

- **Shared Consensus Security**: Both Polkadot and Super Bitcoin's multi-chain networks achieve shared consensus security, but Polkadot shares DOT consensus, while Super Bitcoin shares Bitcoin consensus. The strength of BTC's consensus is far greater than that of DOT. Theoretically, the security of the Super Bitcoin architecture is 200 times higher than that of the Polkadot network. This "200 times" represents the current ratio of BTC's $1.3 trillion market cap to DOT's $6.5 billion market cap. Therefore, the Lightning Chains on Super Bitcoin offer approximately 200 times the security of Polkadot's parachains.
- **Application Chain Architecture**: Super Bitcoin's lightning chain is deployed with one click based on BEVM-stack, whereas on Polkadot, parachains are deployed via Substrate with one-click.
- **Cross-Chain Communication Protocol**: Super Bitcoin uses **lightning channels** as the communication protocol between Lightning Chains, while Polkadot uses **XCMP** as the communication protocol between parachains.

3. System Architecture



3.1 System Architecture Overview

Super Bitcoin is a five-layer architecture protocol built by BEVM guided by the three problems of blockchain - decentralization, security and scalability.. This protocol is based on the Bitcoin protocol and utilizes the Lightning Network for efficient peer-to-peer communication. To extend the functionality of Lightning Network nodes, Super Bitcoin integrates Taproot Consensus and combines Bitcoin SPV, Schnorr signatures, MAST contracts, and a BFT PoS consensus mechanism to achieve scalable state management and transaction processing.

On this foundation, Super Bitcoin further integrates multiple virtual machines, including WASM, EVM, SVM, MoveVM, and CairoVM, creating a multi-chain system based on lightning chains that offers a diverse range of smart contract execution environments. This modular framework significantly enhances the system's scalability and flexibility while maintaining the decentralized nature of the Bitcoin network. Importantly, all lightning chains share the Bitcoin network's consensus security, ensuring that the system remains highly secure as it scales.

3.2 Kernel Layer

The Bitcoin network serves as the kernel layer of Super Bitcoin, maintaining the security and irreversibility of the entire system through the Proof-of-Work (PoW) consensus mechanism. This decentralized peer-to-peer electronic cash system primarily supports BTC transfers and basic opcode execution, managing state using the UTXO model. The Bitcoin network’s block structure and transaction data serve as the input for the Lightning Network, providing reliable

foundational data for the upper layers. Although Bitcoin's scripting system is not Turing-complete, it can support the most basic smart contract functionality through stack-based operations, conditional checks, and cryptographic functions. The network maintains a block time of approximately 10 minutes using a difficulty adjustment algorithm and uses Merkle tree structures to optimize transaction verification efficiency. The security and decentralization of this foundational layer provide a robust consensus security foundation for the entire Super Bitcoin architecture, while its simple design and limited scripting capabilities offer a stable and predictable environment for upper-layer expansion.

3.3 Communication Layer

The Lightning Network serves as the communication layer of Super Bitcoin, achieving efficient asset information transmission while sharing the BTC consensus security. It acts as a bridge between users and the Super Bitcoin ecosystem, enabling bidirectional payment channels through a Hashed Time Lock Contract (HTLC), supporting multi-hop routing and atomic swaps. Users can establish state channels with Super Bitcoin nodes to deposit funds and conduct instant off-chain transactions.

Super Bitcoin nodes, as specialized Lightning Network nodes, not only maintain direct channels with users but also remain compatible with the existing Lightning Network by implementing the BOLT (Basis of Lightning Technology) specifications. This design allows users to leverage the existing Lightning Network infrastructure for cross-node, cross-chain payments and value transfers, providing a secure communication foundation for the lightning chains.

3.4 Extension Layer

Taproot Consensus serves as the extension layer in Super Bitcoin, playing a critical role in connecting the Lightning Network with the upper-layer lightning chains. It abstracts the asset information transmitted through the Lightning Network and converts it into blockchain data that can be processed by the upper layers, balancing the payment efficiency of the Lightning Network with the logical needs of upper-layer applications.

This expansion layer integrates Bitcoin SPV, Schnorr signatures, MAST (Merkelized Abstract Syntax Tree) structures, and a BFT (Byzantine Fault Tolerance) PoS consensus mechanism to achieve multiple functions:

1. **Connecting the Lower Layer**: Bitcoin SPV enables lightweight block header verification, allowing nodes to synchronize with the Bitcoin network in a decentralized manner, providing reliable on-chain data input for the Lightning Network.
2. **Information Processing and Storage**: The PoS-based blockchain network provides distributed storage of Lightning Network channel states. It also processes information for BTC and Taproot Assets, supplying necessary data for upper-layer applications. This mechanism ensures data redundancy and resistance to censorship.
3. **Security Assurance**: Decentralized threshold signatures replace the local key management system of Lightning Network nodes, enhancing key security and flexibility. The aggregation feature of Schnorr Signatures is used to construct a (t, n)

threshold signature network, replacing the traditional single-key management model of the Lightning Network.
4. **Privacy and Complexity**: The MAST structure allows complex conditional scripts to be represented on-chain as a single hash, improving both privacy and script complexity.

Through these mechanisms, the Taproot Consensus extension layer effectively converts verified Lightning Network data into standardized blockchain states. While ensuring security and privacy, it enhances the overall system's performance and scalability. It not only connects the underlying Bitcoin and Lightning Networks but also provides the upper-layer applications with rich and reliable data and functional support.

3.5 Fusion Layer

The Fusion Layer reflects the scalability of Super Bitcoin. It builds on top of Taproot Consensus and utilizes the extensibility of the Substrate framework to achieve a multi-chain interconnected system. Its key features include:

1. **Scalable Multi-Chain Architecture**: Supports the deployment and interconnection of an unlimited number of lightning chains, with BEVM serving as a special lightning chain responsible for managing cross-chain interactions and resource scheduling.
2. **Heterogeneous Compatibility and Standardized Protocols**: Compatible with multiple virtual machines (such as MoveVM, CairoVM, SVM, EVM) and achieves atomic asset exchange and state synchronization through a standardized cross-chain protocol based on the Lightning Network.
3. **Shared Security and Flexible Consensus**: All lightning chains inherit the security of the Bitcoin network, while adopting a pluggable consensus design, with the default being a Taproot-compatible BFT variant.
4. **Ecosystem Expansion**: Facilitates the rapid migration of existing blockchain technologies, extending the decentralized BTC ecosystem to various Turing-complete blockchain applications.

With these features, the Fusion Layer enables Super Bitcoin to evolve into a highly scalable, secure, and interoperable multi-chain ecosystem, providing robust infrastructure support for blockchain innovation.

3.6 Application Layer

The Application Layer is built on top of Super Bitcoin's multi-chain architecture, offering developers a diverse decentralized application (DApp) ecosystem. Leveraging the security, scalability, and interoperability of the underlying layers, it supports the deployment of applications on any Turing-complete virtual machine. Developers can choose to quickly deploy proprietary application chains within the lightning chain framework, or they can deploy various applications directly on the lightning chains. All these applications and chains automatically inherit the consensus and security guarantees of the Bitcoin network.

The Application Layer integrates multiple smart contract execution environments, supporting programming languages such as Solidity (EVM), Move, Cairo, and Rust. The Application Layer lowers the entry barrier for developers and accelerates the innovation cycle. Through standardized API interfaces, developers can utilize Lightning Network channels to achieve decentralized cross-chain asset transfers and information exchanges. Additionally, it incorporates protocols like Taproot Assets, which are compatible with the Lightning Network, further enhancing cross-chain functionality.

Although the services provided by the Application Layer are similar to other VM-based public blockchains, it has two distinctive features: first, it allows the use of decentralized native BTC as the base currency for applications; second, the entire application layer shares the security of the Bitcoin network. Such design not only offers a rich development environment but also ensures that applications are built on solid security and native cryptocurrency support.

4. Shared Consensus Security

Shared BTC consensus security is the security core of our five-layer architecture. This concept is derived from Polkadot's shared security model, which Polkadot defines as Shared Security, also known as Pooled Security, is one of Polkadot's unique value propositions. In essence, it means that all parachains connected to Polkadot's relay chain benefit from the full security of the entire Polkadot network.

Our five-layer protocol architecture further extends this concept by leveraging the Bitcoin (BTC) network—currently recognized as the most secure blockchain consensus system—to ensure the security of the entire ecosystem. Compared to Polkadot's parachains, which share Polkadot's consensus security, our architecture is directly built on top of the Bitcoin network, sharing Bitcoin’s consensus security.

Existing BTC Layer2 solutions typically ensure security through cross-chain mechanisms or BTC staking, which only utilize part of Bitcoin’s consensus security. In contrast, our five-layer protocol is built on the Lightning Network, using HTLC (Hashed Timelockd Contract) and commitment transactions, with security fully dependent on BTC consensus. This design allows our system to fully inherit the consensus security of the Bitcoin network.

Specifically, our architecture achieves shared BTC consensus security through the following methods:

1. Leveraging the peer-to-peer channels of the Lightning Network to ensure that all transactions are ultimately settled on the Bitcoin mainnet.
2. Using HTLC commitment transactions, where each state update is protected by the consensus of the Bitcoin network.
3. Through the Taproot Consensus extension layer, extending Bitcoin's security features to more complex smart contract environments.
4. In the multi-chain system, all lightning chains share Bitcoin’s network consensus security, ensuring consistency and reliability across the entire ecosystem.

5. Lightning Chain

Based on the shared BTC consensus security, we utilize the lightning chain to create a Value Internet. To achieve this, the architecture of the lightning chain network is inspired by Polkadot's relay chain and parachain design:

1. **Relay Chain**: It serves as the central nervous system of the entire network, responsible for the overall security, cross-chain communication, and consensus mechanism. The relay chain does not execute specific application logic but focuses on coordinating the operations of the entire ecosystem.
2. **Parachains**: These are independent blockchains that run in parallel with the relay chain. Each parachain can have its own token economy and governance mechanism, achieving interoperability through the relay chain and sharing the security guarantees provided by the relay chain.

Drawing from Polkadot’s design, Super Bitcoin proposes a multi-chain interoperability system based on Bitcoin and the Lightning Network. In this system, the **Lightning Chain** functions similarly to Polkadot's parachains, with the following unique characteristics:

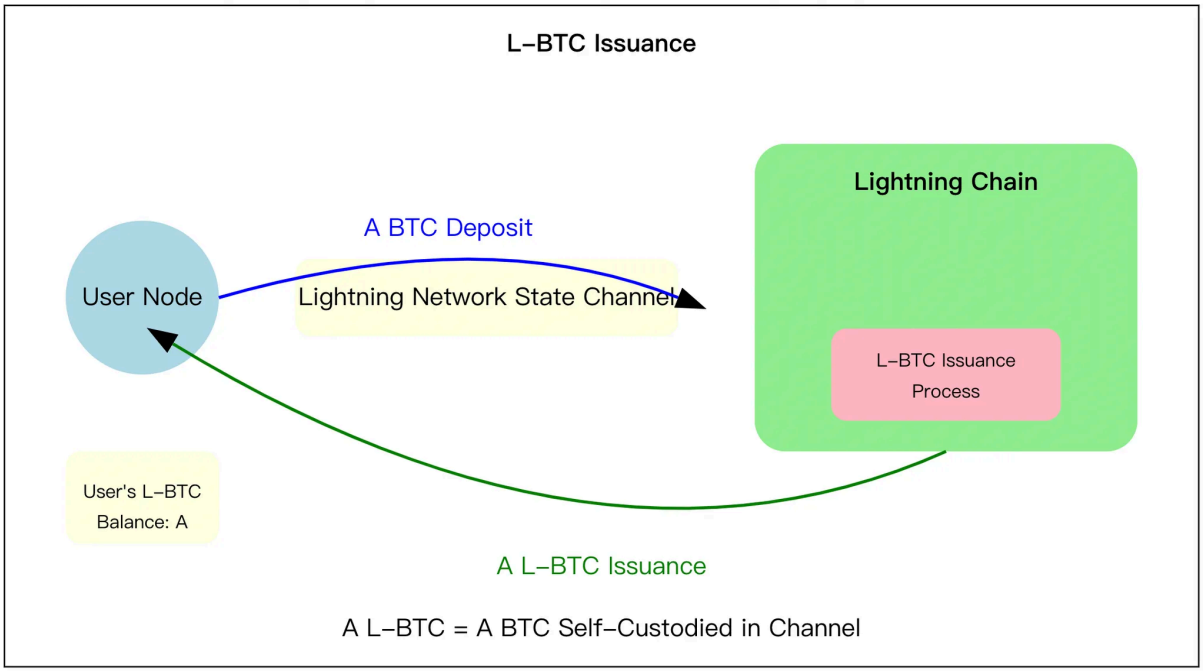
1. **Shared BTC Consensus Security**: Unlike Polkadot’s independent consensus model based on PoS staking, Lightning Chain directly inherits the consensus security of the Bitcoin network, providing unprecedented security for the entire ecosystem.
2. **Lightning Network Integration**: Lightning Chain deeply integrates Lightning Network technology, enabling high-speed, low-cost transaction processing, significantly enhancing the throughput and efficiency of the entire system.
3. **Scalability**: Theoretically, an unlimited number of Lightning Chains can be deployed, with each Lightning Chain optimized for specific application scenarios or industry needs, offering a high degree of flexibility and scalability.
4. **BEVM as the Core Coordinator**: In this ecosystem, BEVM (Bitcoin-Enhanced Virtual Machine) acts as a special Lightning Chain, playing a role similar to that of Polkadot’s relay chain. It is responsible for the governance and resource allocation of the entire network, ensuring efficient collaboration between different Lightning Chains.
5. **Shared Lightning Network Liquidity**: All Lightning Chains share the same Lightning Network, which means they can access a common liquidity pool, improving capital efficiency.

These features not only highlight the innovative design of Lightning Chain but also underscore its fundamental differences from existing BTC Layer 2 solutions. By directly sharing Bitcoin network consensus security and Lightning Network liquidity, Lightning Chain achieves a qualitative leap in both security and interoperability.

5.1 Lightning Chain

The Lightning Chain is the core component of Super Bitcoin that directly interacts with users. Its main responsibilities include handling user transactions, managing asset mapping, and executing smart contracts.

5.1.1 BTC Asset Mapping

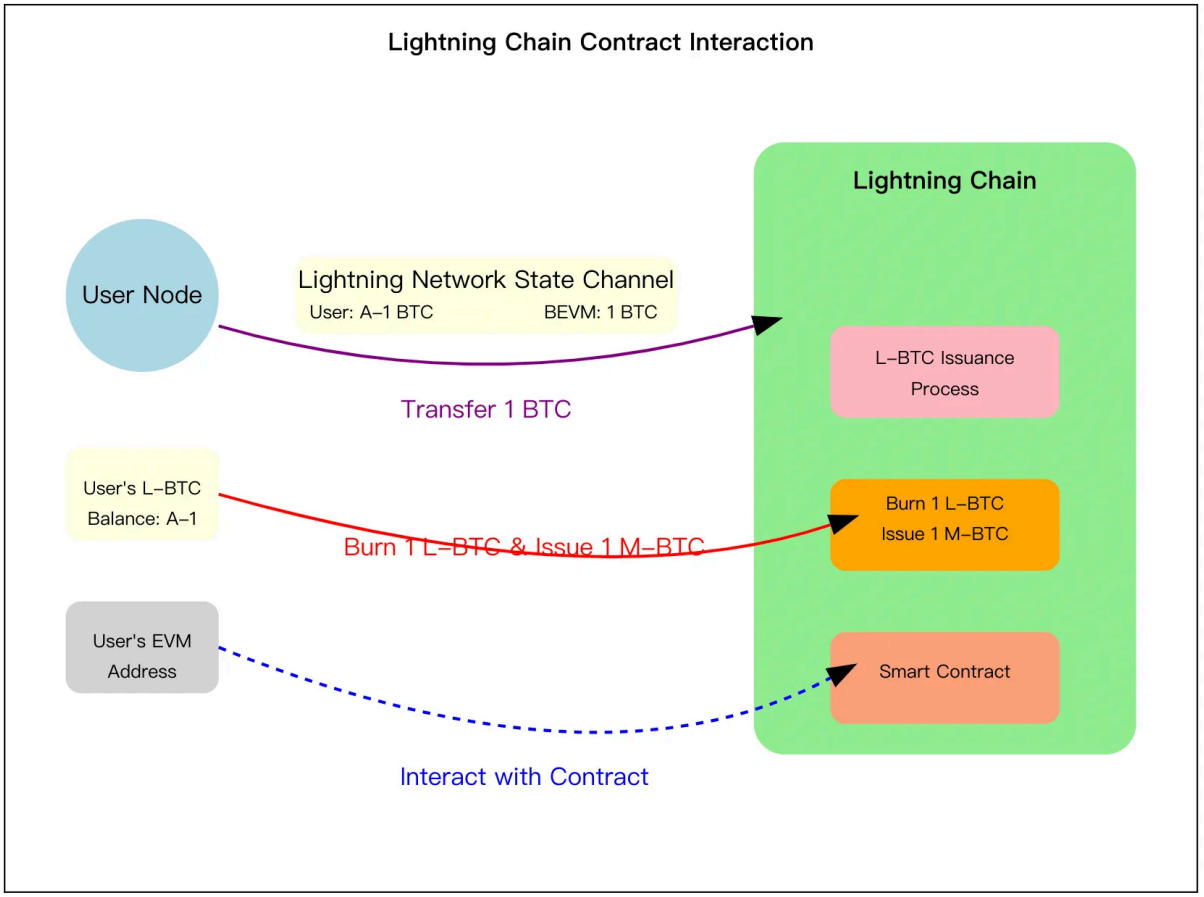


Lightning Chain functions as both a node in the Lightning Network and a PoS (Proof of Stake) network. In this system, BTC is locked within the Lightning Network, while **L-BTC** represents the user's BTC balance in their Lightning Chain account. The mapping process between these two ensures the consistency and security of the assets. The specific BTC-to-L-BTC mapping process is as follows:

1. The user establishes a channel with the Lightning Chain via the standard Lightning Network protocol.
2. The user deposits **A** BTC into the Lightning Network channel.
3. As the Lightning Chain operates as a PoS network, the validators within the network observe this new BTC deposit.
4. Once more than two-thirds of the validators reach consensus and confirm the BTC deposit event, the Lightning Chain will issue **A** L-BTC accordingly.

This process ensures that the issuance of L-BTC always maintains a 1:1 ratio with the BTC locked in the Lightning Network channel. It's important to note that L-BTC is self-custodied by the user, so there is no need to worry about asset security. Additionally, PoS consensus here is not used to secure L-BTC assets but acts as a distributed ledger for the state of the Lightning Network channel, solving the potential issue of data loss in local storage by Lightning Network nodes.

5.1.2 Smart Contract Interaction on the Lightning Chain

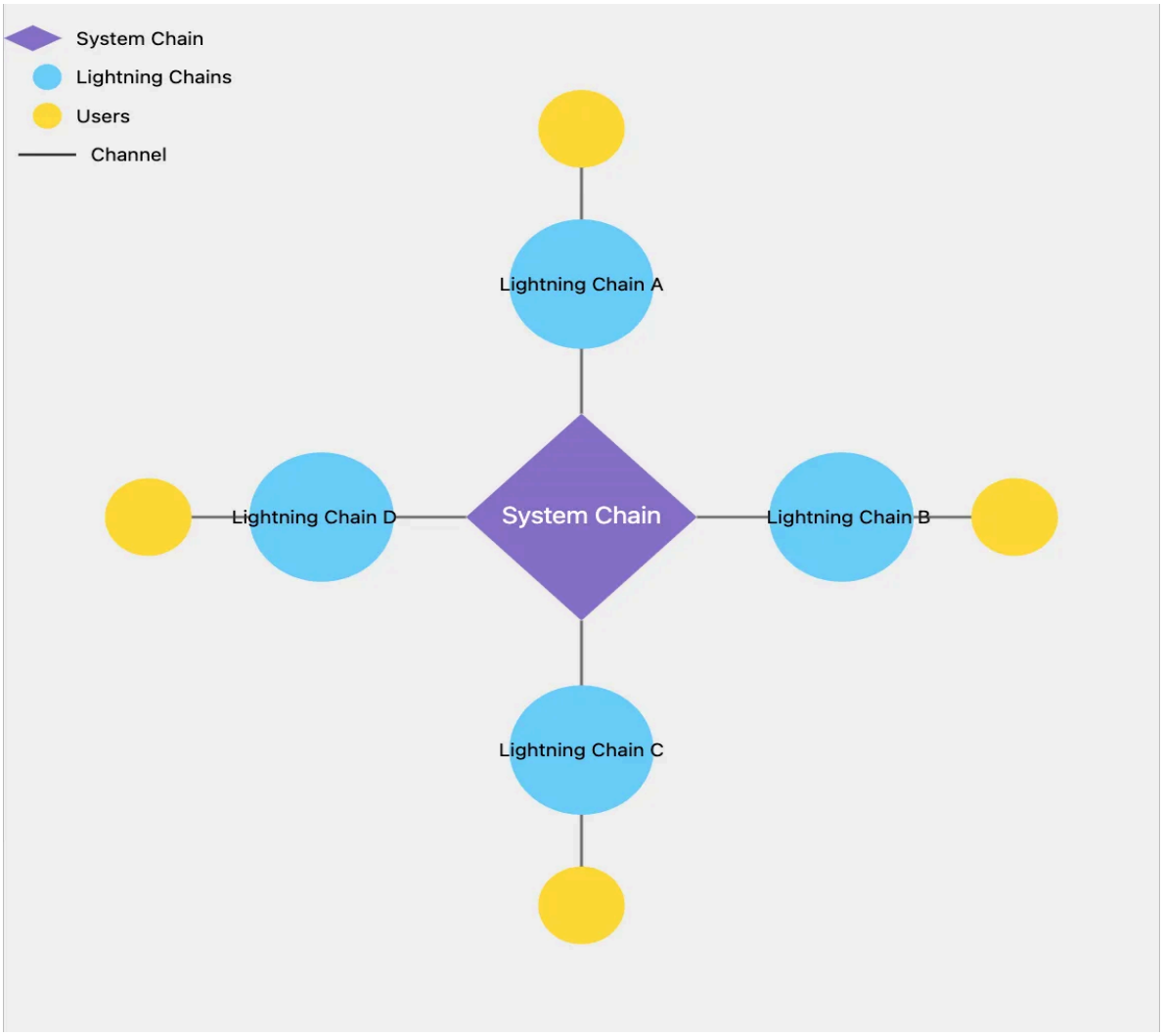


Interaction with smart contracts on the **Lightning Chain** follows a "authorize first, execute later" paradigm. In this process, users need to convert **L-BTC** into **M-BTC**, where M-BTC represents the asset that can interact with smart contracts on the Lightning Chain. The specific interaction process is as follows:

1. **Asset Preparation**: The user holds **A** BTC in the Lightning Network state channel and decides to interact with a smart contract using 1 BTC.
2. **Authorization Operation**: The user authorizes the Lightning Chain network to convert 1 L-BTC into 1 M-BTC. This step does not immediately execute the conversion but provides the necessary permissions for subsequent interactions.
3. **Smart Contract Invocation**: The user initiates a smart contract call, specifying the use of 1 M-BTC. The Lightning Chain network checks the authorization and, upon confirming its validity, performs the following actions: destroys 1 L-BTC from the user’s balance, mints 1 M-BTC, and uses it directly for interaction with the smart contract.
4. **Transaction Execution**: The smart contract executes the specified operation using the minted M-BTC.

This process enables the seamless application of Bitcoin assets within a smart contract environment while maintaining a clear separation between L-BTC, which functions as channel liquidity, and M-BTC, which serves as a medium for contract interaction.

5.2 System Chain



System Chain is the core coordination component of Super Bitcoin implemented through the upgraded BEVM (Bitcoin-Enhanced Virtual Machine). As a special Lightning Chain, it establishes direct connections with all regular Lightning Chains in the network, forming an efficient star topology structure. This design makes the System Chain the central hub of Super Bitcoin.

The System Chain is primarily responsible for incentivizing Lightning Network nodes and coordinating cross-chain interoperability, effectively managing the entire network to ensure its efficient operation. In terms of node incentives, the System Chain implements a complex and sophisticated mechanism. It uses a dynamic reward algorithm that adjusts reward distribution based on the activity level, liquidity provided, and overall contribution to the network. During this process, the System Chain considers multi-dimensional evaluation metrics, such as the node's uptime, transaction throughput, and routing efficiency.

In terms of cross-chain interoperability, the System Chain plays a key coordination role, facilitating seamless interactions between different Lightning Chains. It implements a secure cross-chain communication protocol based on Hashed Time Lock Contract (HTLC), ensuring the security and reliability of message transmission. Additionally, the System Chain introduces an atomic swap mechanism, which effectively prevents potential loss of funds during cross-chain asset transfers. Furthermore, by defining a unified cross-chain asset

standard, the System Chain simplifies the asset mapping process between different Lightning Chains, further improving the efficiency and convenience of cross-chain operations.

6. Economic Model

The economic model of BEVM (Bitcoin-Enhanced Virtual Machine) combines Bitcoin's issuance mechanism with the functional characteristics of the Lightning Network. It aims to address the sustainable competitiveness of Super Bitcoin and provide a long-term incentive system for the Lightning Network.

At the core of this model is the combination of Lightning Network node incentives and a staking-mining mechanism. Lightning Network nodes that establish state channels with the BEVM network can participate in staking mining. Staking mining uses a Verifiable Random Function (VRF) to determine mining probabilities, rather than distributing rewards proportionally based on the staked amount.

During the staking mining process, participants stake BTC in state channels, and the system calculates the mining probability based on the VRF. For example, if three nodes stake 100 BTC, 10 BTC, and 1 BTC, their respective mining probabilities would be 90.09%, 9.01%, and 0.90%. This mechanism ensures that smaller stakers also have a substantial opportunity to earn rewards.

A dedicated whitepaper on the economic model will be released for this section, so this document will not go into further details.

7. Future Development

7.1 Short-Term Goals

The short-term goals of Super Bitcoin focus on implementing core functionalities and building the necessary infrastructure. By realizing the proposed five-layer protocol, we will introduce smart contract functionality based on the Lightning Network while sharing BTC consensus security. For users, participating in Super Bitcoin ensures that the BTC they hold remains fully under their control. At the same time, they will be able to use BTC, Taproot Assets, and other native assets within smart contracts.

7.2 Long-Term Vision

The long-term vision of Super Bitcoin is to build a global Value Internet that shares BTC consensus security. We aim to design an incentive mechanism through an innovative economic model, promoting widespread use of Lightning Network nodes. Furthermore, we are committed to deeply integrating existing blockchain ecosystems with Super Bitcoin, enabling the free flow and interaction of BTC assets. By doing so, we aim to create a secure,

efficient, and interoperable blockchain ecosystem where BTC becomes the core, and all blockchain consensus models share the security of the Bitcoin network. Ultimately, our goal is to enable the Bitcoin network to scale infinitely while maintaining decentralization.

7.3 Potential Challenges and Solutions

Super Bitcoin faces several potential challenges in achieving its goals. Transforming Lightning Network nodes into a full-fledged network involves complex technical challenges that require extensive testing. Another challenge is designing a better economic incentive model to attract enough Lightning Network node operators to adopt Super Bitcoin. Ensuring seamless communication and atomic swaps between different node networks is also crucial, and the team will focus on developing standardized protocols and interfaces to enhance network interoperability. As the system’s complexity increases, maintaining network security will become more challenging. Super Bitcoin will adopt rigorous security audit processes and consider introducing advanced cryptographic technologies to strengthen system security. As the number of lightning chains grows, managing the state and interaction between networks may pose scalability challenges. By actively addressing these challenges, Super Bitcoin aims to bring revolutionary changes to the Bitcoin and Lightning Network ecosystems, creating a more flexible, efficient, and scalable infrastructure.

8. Conclusion

The five-layer architecture introduced by Super Bitcoin not only solves the problem of existing BTC Layer 2 solutions not being able to share Bitcoin's consensus security but also addresses the limitation of the Lightning Network being restricted to payment scenarios. It perfectly combines the shared BTC consensus security with smart contract functionality. Our protocol uses the Bitcoin network as the core, ensuring the highest level of security. It leverages the Lightning Network to construct an efficient communication layer, significantly improving scalability and flexibility while preserving the security of the native BTC consensus. By introducing Taproot Consensus as the extension layer, it abstracts Bitcoin and Lightning Network data to provide actionable data for the upper layers. Through the multi-chain fusion layer formed by lightning chains, we achieve a "multi-chain interconnection" supporting the free flow of cross-chain assets. The application layer offers developers a rich set of tools, fostering the development of a diverse DApp ecosystem. Combined with the innovative VRF-based staking mining mechanism, Super Bitcoin adds an incentive layer to the Lightning Network and allows the decentralized Bitcoin network to have unlimited flexibility and scalability.

9. References

[1] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf

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

[3]Habermeier, S., et al. (2020). "Substrate: A modular framework for building blockchains." https://www.parity.io/substrate/

[4]Wuille, P., Nick, J., & Towns, A. (2019). "Taproot: SegWit version 1 spending rules." https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki

[5] Nick, J., Seurin, Y., & Wuille, P. (2020). "Schnorr Signatures for secp256k1." https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki

[6]Wood, G. (2016). "Polkadot: Vision for a heterogeneous multi-chain framework." https://polkadot.network/PolkaDotPaper.pdf