OpenBit - Pump Liquidity in Bitcoin

Version: Beta

OpenBit Team

Abstract—**Bitcoin's inception marked a milestone in blockchain history, yet its liquidity remains disproportionately low due to inherent network limitations, in contrast to its significant value and consensus in the market. Despite upgrades like SegWit and Taproot, Bitcoin struggles to explore its full potential in blockchain applications. This white paper introduces OpenBit, a cross-bitcoin liquidity infrastructure designed to address the liquidity challenges within the Bitcoin ecosystem. OpenBit leverages cryptographic technologies, including Trusted Execution Environments (TEE) and Zero-Knowledge Proofs (ZKP), to provide a secure and efficient cross-chain liquidity solution. We present OpenBit's technical architecture, node governance mechanisms, and user journey, highlighting its role as a universal cross-chain liquidity infrastructure for the Bitcoin ecosystem.**

Index Terms—**Bitcoin, Trusted Execution Environment, Zero Knowledge Proof, Cross-Chain Bridge, L2 blockchain, EVM, smart contracts, security.**

I. Introduction

Originating from Satoshi Nakamoto's groundbreaking white paper in 2008 [1], Bitcoin disrupted the economy by enabling trustless cross-border financial transactions without intermediaries. Its core principles, such as censorship resistance, immutability, and decentralization, have remained fundamental. Despite Bitcoin's protocol limitations, Ethereum emerged as a notable alternative [2], introducing smart contract capabilities that propelled a technological leap and fostered a diverse range of decentralized applications. Post-2020, Ethereum solidified its position with the emergence of DeFi and NFTs, alongside other smart contract platforms like Solana [3] and Avalanche [4]. Nevertheless, Bitcoin has upheld its primary role as digital gold, underscoring its unparalleled value and consensus in the blockchain ecosystem.

Over the past few years, Bitcoin price has surged dramatically, but its liquidity remains disproportionately low due to inherent limitations in the Bitcoin network. Insights from Glassnode highlight concerns about Bitcoin's liquidity, with approximately 69% of the circulating supply inactive for over a year. Despite upgrades like Segregated Witness (SegWit) [5] and Taproot [6] [7] [8] aimed at enhancing performance and functionality, Bitcoin still struggles to explore diverse use cases within its ecosystem.

With Bitcoin's fourth halving, miners face reduced income, challenging the security of the Bitcoin network reliant on miners. The emergence of Bitcoin inscriptions has brought in significant revenue streams for miners but has also introduced new challenges. Consequently, Bitcoin scaling solutions and asset issuance schemes on top of Bitcoin have become crucial areas of development.

The rise of inscriptions [9], the flourishing of Bitcoin's EVM L2, and the imminent upgrade of Bitcoin scaling solutions mark a period of exploration for Bitcoin asset issuance, scalability, and interoperability. With the increasing utility scenarios for Bitcoin, the revenue structure of miners will gradually evolve, providing greater economic incentives for this development.

In this developmental process, OpenBit emerges as a solution to address the liquidity challenges in BTC. Designed to integrate with the existing ecosystem seamlessly, OpenBit aims to deliver a user-friendly liquidity solution. It facilitates the smooth movement of assets within the Bitcoin ecosystem and onto other blockchains while minimizing barriers to new capital entry. By enabling unrestricted asset and capital movement, OpenBit seeks to maximize the potential of the Bitcoin ecosystem.

II. Background

The Bitcoin network faces significant challenges, particularly concerning scalability and the development of decentralized applications (DApps) built on top of Bitcoin. These challenges hinder the flow of Bitcoin assets across different blockchains and the establishment of a robust decentralized application ecosystem. To address these issues, various scalability solutions have been proposed and implemented. Additionally, the emergence of cross-chain infrastructure solutions aims to facilitate the movement of assets between Bitcoin and other blockchains, though current options are limited.

A. Challenges

1) Scalability: Bitcoin faces persistent constraints in state, computation, and verification, hindering its ability to process substantial transaction volumes efficiently. Various scalability solutions, including state channels, sidechains, and client-side validation, have been proposed to address these limitations.

- State Channels:
  State channels create direct channels between two or more transaction participants, allowing them to conduct multiple transactions rapidly within the channel without requiring confirmation for each transaction on Bitcoin. The Lightning Network [10] is a prominent example of a state channel solution designed to address Bitcoin's scalability issues and high transaction fees. By establishing bidirectional payment channels, the Lightning Network enables users to conduct fast and low-cost transactions outside the Bitcoin main chain. However, the Lightning

Network primarily caters to small-scale payments and transfers due to capacity limitations.

- Sidechains:
  Bitcoin sidechains are independent blockchains connected to the Bitcoin itself, enabling users to transfer assets between them. Stacks [11] and Liquid [12] are examples of sidechain solutions aiming at enhancing Bitcoin's functionality. Stacks provides a smart contract layer for Bitcoin and facilitates cross-chain interactions, while Liquid focuses on rapid, high-value, and anonymous transfers for exchanges and trading platforms. However, issues of centralization persist in most sidechain solutions, limiting their ecosystem development.
- Client-side Validation:
  Client-side validation schemes continue the UTXO model, allowing off-chain clients to handle more complex transactions. RGB [13] is a Bitcoin Layer 2 protocol built upon Bitcoin's UTXO and Lightning Network infrastructure. While RGB offers scalability, privacy, and programmability benefits, it faces challenges in verification complexity and blockchain security. The market acceptance and feasibility of RGB require further examination and validation.

2) Programmability: Given Bitcoin's current limitations in programmability, notably due to its simplistic scripting language, developers encounter significant hurdles in expanding the ecosystem beyond its native capabilities. The language's constraints limit the sophistication of decentralized applications (DApps) that can be built directly on the Bitcoin blockchain.

The surge in Bitcoin scaling solutions and staking solutions reflects a concerted effort to address the limitations of Bitcoin's programmability. Projects such as Rootstock (RSK) [14] and BEVM [15] exemplify this trend by offering EVM-compatible environments within the Bitcoin ecosystem. These environments facilitate the execution of smart contracts on Bitcoin, providing developers with access to Ethereum-like functionalities while capitalizing on the security and network effects of Bitcoin. These initiatives expand Bitcoin's utility and attract developers familiar with Ethereum's programming model, thereby addressing programmability challenges while enhancing the overall Bitcoin ecosystem.

Despite these advancements in expanding Bitcoin's programmability, the ecosystem still faces a critical challenge: Bitcoin's native assets cannot seamlessly flow across different blockchain ecosystems. This limitation restricts BTC holders from accessing the liquidity benefits and diverse financial instruments available in other blockchain networks. Therefore, there is a pressing need for further innovation to enable the seamless movement of Bitcoin's native assets and unlock liquidity opportunities for Bitcoin holders across various blockchain ecosystems.

3) Cross-Chain Infrastructure: Currently, the transfer of value from the Bitcoin blockchain to other chains, and vice versa, poses a significant challenge. To address this, there are primarily two main approaches for facilitating Bitcoin's assets transfer: centralized exchanges (CeFi) and bridges supporting Bitcoin cross-chain transactions.

- Centralized Exchanges
  Cross-chain transactions through centralized exchanges involve platforms such as Binance's bBTC. Notably, Binance locks a portion of tokens on its native chain and mints an equivalent number of ERC20 tokens on Ethereum, denoted as bBTC. However, the primary drawback lies in the centralized nature of these exchanges, requiring users to place trust in them.
- BTC-supporting bridges
  BTC-supporting bridges, exemplified by projects like Polyhedra [16], Cobo, and Liquid [12], offer another avenue. Each employs unique mechanisms, but they face distinct challenges. For instance, Pos-Based Bridges like Thorchain [17] and Polyhedra rely on staking mechanisms and user-initiated reporting for security, leading to extended waiting times for committee operations. Meanwhile, MPC-Based Bridges like Cobo depend on real-world security companies, resulting in costly transaction frictions and requiring users to undergo centralized and cumbersome Know Your Customer (KYC) procedures. Additionally, Sidechain-Based solutions like the Liquid Network [12] only support transactions between Bitcoin and its sidechains.

In the market, there exists a demand for a product that can provide robust security, low costs, and a seamless user experience simultaneously.

III. OpenBit's Position in Bitcoin ecosystem

OpenBit functions as the Bitcoin ecosystem's liquidity layer, forging strong connections with diverse stakeholders and delivering distinct value to each. It serves as a vital cross-chain DeFi infrastructure within the Bitcoin ecosystem. Specifically, for Bitcoin assets, where liquidity and usage beyond long-term holding are key challenges, OpenBit enables seamless bridging and swapping of diverse Bitcoin assets across chains. This facilitates their trading, investment, and integration into other ecosystems, thereby enhancing liquidity. For Bitcoin layer 2 solutions, which struggle to transcend the Bitcoin ecosystem despite their potential to lower trading barriers, OpenBit bridges their assets across chains, further boosting liquidity. Additionally, for Bitcoin sidechains, Ethereum, and other chains, which lack association with the Bitcoin ecosystem and miss out on Bitcoin's growth opportunities, OpenBit acts as a gateway, converting Bitcoin assets into compatible assets for their chains.

IV. Technical Perspectives

This section provides a technical overview of OpenBit and its architecture. OpenBit is the industry's first pure programming- and mathematics-based fully on-chain Bitcoin DeFi solution. We use cryptographic technologies, efficiently bridging assets across multi-chains with TEE(trusted execution environment) [18] and safely scaling DeFi application with Zero-Knowledge Proof (ZKP) [19]. We also relax the Trusted

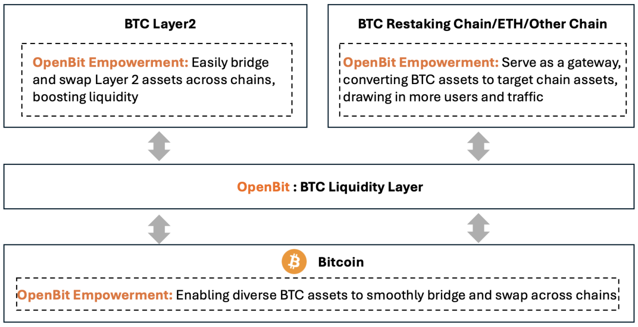

BTC Layer2
OpenBit Empowerment: Easily bridge and swap Layer 2 assets across chains, boosting liquidity
BTC Restaking Chain/ETH/Other Chain
OpenBit Empowerment: Serve as a gateway, converting BTC assets to target chain assets, drawing in more users and traffic
OpenBit : BTC Liquidity Layer
Bitcoin
OpenBit Empowerment: Enabling diverse BTC assets to smoothly bridge and swap across chains

Figure 1. OpenBit in Bitcoin Ecosystem

Execution Environment's (TEE) centralized trust assumption by introducing our innovative De-TEE Network. The system comprises four main components: a De-TEE network, an Execution layer, a DA Layer, and a set of Ethereum L1 contracts. In principle, our design as a universal cross-chain liquidity solution may be applied to any blockchain pairs, including Bitcoin, Ethereum, and even other non-EVM blockchain We will introduce them using Bitcoin and Ethereum for example in the following subsections

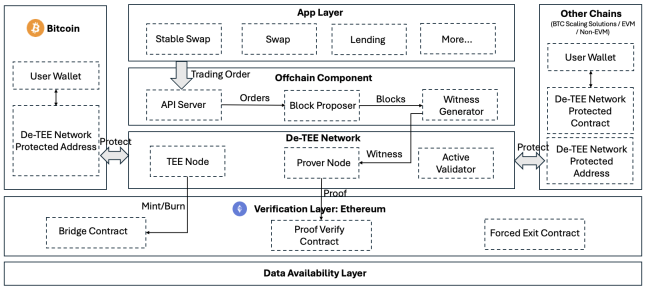


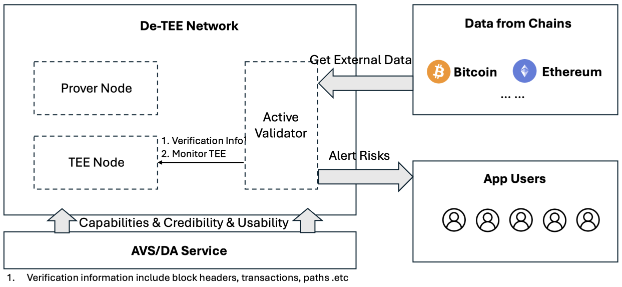
Figure 2. System Architecture

A. De-TEE network

The De-TEE network in our system functions as a universal cross-chain bridge.

It securely generates and stores the private keys of the Bitcoin deposit address and private keys of the Bridge Contract, and it runs the key control program and transaction verification program within its enclave. The programs run inside the TEE are open-sourced and everyone can verify their runtime integrity against the remote attestation. Different from other TEE-based solutions, in our De-TEE network, each TEE node contains TEEs from multiple TEE hardware manufacturers, effectively avoiding the additional centralized trust assumption introduced by a single TEE vendor. Furthermore, we also introduce Active Validators to ensure the validity of external data feed in the TEE environment.

As shown in figure 3, the De-TEE network consists of three major components: TEE Nodes, Prover Nodes, and Active Validators (AVs).



1. Verification information include block headers, transactions, paths .etc

Figure 3. De-TEE Architecture

1) TEE node: The TEE node is one of the core parts of OpenBit's De-TEE network. OpenBit leverages TEE nodes from various vendors to form its TEE network. These nodes collectively establish a distributed network, enabling parallel processing of sensitive tasks and facilitating the necessary sharing of private data through remote attestation mechanisms. There are two major programs built in the TEE node.

- *Keys Generation Program:* This program generates users' deposit addresses and corresponding private keys for Bitcoin and public and private keys used in OpenBit's Ethereum L1 contracts. Deposit addresses and public keys are included in remote attestation reports and published on OpenBit's website, while private keys are encrypted by keys embedded within TEEs and backed up across multiple TEE nodes.
- *Keys Control Program:* This program retrieves block headers from various data sources, including Active Validators, to the enclave of TEE to ensure header accuracy. Subsequently, it obtains corresponding on-chain transactions and Merkle paths from AVs, and after validating the transactions within the TEE, it utilizes controlled private keys to sign users' deposit and withdrawal operations. A transaction will pass if the whole TEE network passes a threshold signature.

The remote attestation reports, along with the programs' source code, deposit addresses, and public keys, will be publicly available on the OpenBit website. Anyone can obtain the remote attestation report and interact with TEE providers' (Intel SGXArm TrustZoneAWS Nitr etc.) servers to verify the authenticity of the report.

2) Prover Node: The Prover nodes receive tasks from Witness Generators in execution layers and compute zero-knowledge proof (PLONK) [20] for that block, and send that proof to the Proof Verification Contract on Ethereum to verify all transactions executed on off-chain Execution Layer are valid and cryptographically equivalent to transactions on Ethereum.

3) Active Validator: Active Validators in the De-TEE network ensure the credibility and availability of external data that enters the TEE enclave within the OpenBit De-TEE network. AVs provide transaction data including block headers and transaction paths for TEE to verify the authenticity and validity of transactions. They also actively monitor the remote attestation reports posted on OpenBit's website and warn of any abnormal behaviors. AVs will be rewarded with tokens for feeding data truthfully and get punished for untruthful information.

B. Execution Layer

The Execution layer in OpenBit serves as a trading engine for various DeFi applications. The execution layer can be abstracted into two logical components:

- *Block Proposer*: Responsible for receiving transaction requests initiated from the application layer, performing preliminary legality checks, and assembling transactions into off-chain blocks.

  A transaction may come into the Execution layer from Application Layer(such as Stable Swap and Lending) or Ethereum L1(Deposit, Withdraw). StateKeeper in Block Proposer regularly forms off-chain blocks and executes them. These blocks consist of transactions from Ethereum L1 and Application Layer, sorted based on priority and time of receipt, with Layer 1 transactions having higher priority. If an L2 block meets the conditions of being a full block, the root hash of the block is calculated and persisted, awaiting on-chain submission. Otherwise, it is stored as a pending block, waiting to be converted into a full block later.

  The AggregatedCommitter aggregates the already formed full blocks into corresponding Ethereum operations according to three types: Commit, Prove, and Execute, awaiting on-chain submission, verification, and execution. Eth Sender reads these operations and calls the main OpenBit contracts.
- *Witness Generator*: Converts off-chain blocks into inputs for Prover Nodes in De-TEE network, enabling Prover Nodes to generate PLONK proofs.

  The Witness Generator and Prover periodically generate witnesses and proofs for the full blocks of L2. Only after generating proofs can the AggregatedCommitter in Block proposer aggregate Prove and Execute operations.

C. DA Layer

the DA layer will store the pub data of off-chain block transactions to reduce gas costs. The contracts on Ethereum will link the information submitted by the DA layer and the block generated by the Execution layer.

D. Ethereum L1 contracts

There are three major contracts deployed on Ethereum L1. Bridge Contract, Proof Verification Contract, and Forced Exit Contract. They serve different functionalities and complete the architecture with other components of OpenBit.

- *Bridge Contract* Controlled by TEE nodes within the De-TEE Network, this contract handles minting and burning bridged tokens on the Ethereum. Once the TEE nodes hear events such as deposits and withdrawals on the Bitcoin and verify validity, they invoke the Bridge contract to execute corresponding minting and burning operations.
- *Proof Verification Contract* verifies PLONK proof generated by Prover Nodes in De-TEE network and updates the global state if the proof is accepted.
- *Forced Exit Contract* allows users to fully extract their tokens in case OpenBit's services fail to work

V. Node Governance

We design node governance mechanisms to manage the De-TEE network nodes

A. Joining the network

Any external individual or organization can join the De-TEE network to serve as one or more types of De-TEE nodes (TEE nodes, Prover Nodes, or Active Validators) as long as they satisfy the admission requirements. Specifically, to become a TEE node, it has to run one of the De-TEE-supported TEE hardware (Intel SGX, Arm TrustZone, AWS Nitro), and to become a Prover node, it must meet the hardware specifications listed on OpenBit's website (will be published before the mainnet launch)

B. Reward and Punishment

OpenBit will reward participating nodes with tokens. TEE nodes may claim rewards if they truthfully fulfill bridging tasks with results agreed with other TEE nodes. Prover nodes may receive rewards if they finish proving tasks timely with proof accepted by the Verification Contract.

OpenBit will also punish inactive nodes and malicious nodes. If a node fails to complete its assigned task within the specified time, it is deemed ”inactive”. When the number of times a node becomes ”inactive” reaches the threshold, it permanently loses its qualification to be a node.

OpenBit has zero tolerance for malicious nodes. Once a node is found to be malicious, it permanently loses its qualification to be a node. For TEE nodes, if their cross-chain results are not recognized by other types of TEE nodes, they are considered malicious. For proof nodes, if the proofs they generate are rejected by Verification Contracts, they are also considered malicious.

VI. Key Advantages

We argue that OpenBit possesses the following desirable advantages:

1) **Safe** OpenBit's security design only relies on mathematics and open-source code. Everyone can verify its computation, and it introduces no additional trust assumption.
2) **Universal** OpenBit supports all kinds of on-chain assets across different blockchains, including EVM, non-EVM, Bitcoin, and other major L1/L2 chains.
3) **Efficient** OpenBit employs ZKP as a DeFi application scaling solution and De-TEE as an on-chain assets bridge across multi-chains, offering several orders of magnitude performance improvement over Ethereum L1.

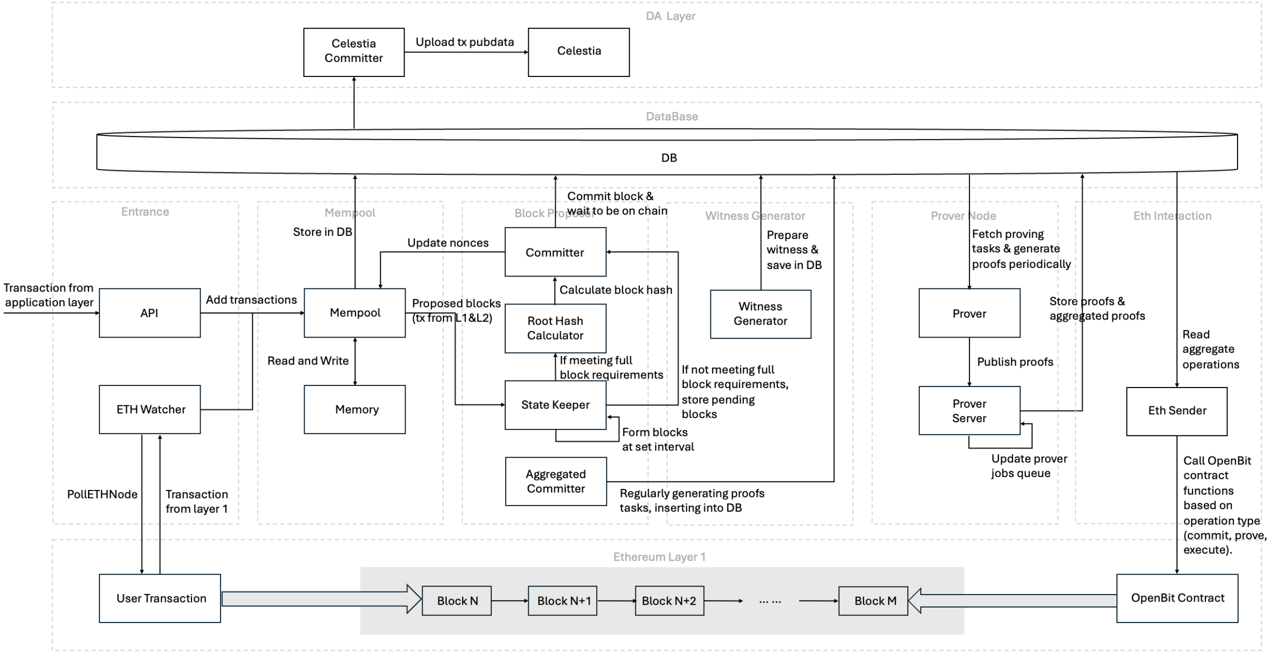


Figure 4. Execution Layer

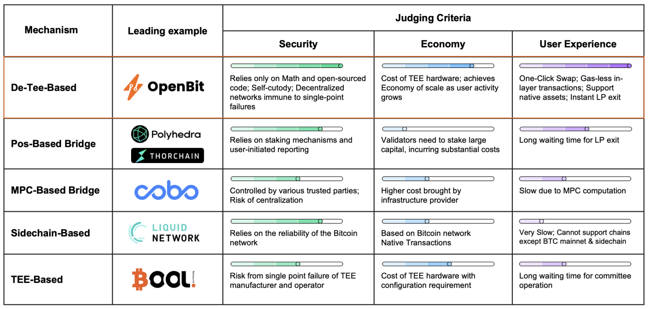
4) **Economic** Different from traditional multi-chain solutions, OpenBit only pushes ZKP to Ethereum and thus saves more gas.
5) **Decentralized** TEE nodes in OpenBit's De-TEE Network contain TEEs from multiple providers, effectively avoiding single-point failure and the additional trust assumption introduced by single TEE providers.
6) **Fast** OpenBit allows users to withdraw their assets instantly, much faster than staking-based solutions which usually take days to withdraw.
7) **Data Available** OpenBit flexibly accommodates zk-rollup, Validium, and dedicated DA layers like Celestia DA.

VII. Key Features

A. A Cross-Bitcoin Infrastructure

We evaluated various technical solutions for bridging within the Bitcoin ecosystem, considering their strengths and limitations:

- The PoS-based Bridge approaches, exemplified by projects like Polyhedra [16] and THORCHAIN [17], relies on staking mechanisms and user-initiated reporting for security. However, this necessitates validators to stake significant capital, resulting in substantial costs and potentially long waiting times for Limited Partners (LP) exit.
- MPC-based Bridge solutions, such as Cobo, involve various trusted parties, risking centralization. Additionally, the computationally intensive MPC process can lead to slower transaction speeds, and higher infrastructure provider costs could further impact user experience.
- Sidechain-based mechanisms, like Liquid Network [12], leverage Bitcoin network reliability for security but are limited to supporting only the Bitcoin and its sidechain pairs, resulting in slow performance not extendable to other chains.
- TEE-based solutions, exemplified by Bool Network [21], face single-point failure risks from the Trusted Execution Environment (TEE) manufacturers and operators. Significant expenses associated with TEE hardware and configuration, along with prolonged waiting periods for committee operations, could potentially hinder user experience.



Mechanism	Leading example	Judging Criteria		
		Security	Economy	User Experience
De-Tee-Based	OpenBit	Relies only on Math and open-sourced code; Self-cutody; Decentralized networks immune to single-point failures	Cost of TEE hardware; achieves Economy of scale as user activity grows	One-Click Swap; Gas-less in-layer transactions; Support native assets; Instant LP exit
Pos-Based Bridge	Polyhedra THORCHAIN	Relies on staking mechanisms and user-initiated reporting	Validators need to stake large capital, incurring substantial costs	Long waiting time for LP exit
MPC-Based Bridge	cobo	Controlled by various trusted parties; Risk of centralization	Higher cost brought by infrastructure provider	Slow due to MPC computation
Sidechain-Based	LIQUID NETWORK	Relies on the reliability of the Bitcoin network	Based on Bitcoin network Native Transactions	Very Slow; Cannot support chains except BTC mainnet & sidechain
TEE-Based	BOOL Network	Risk from single point failure of TEE manufacturer and operator	Cost of TEE hardware with configuration requirement	Long waiting time for committee operation

Figure 5. Comparison Between Different Projects

After careful consideration, we opted for the De-TEE network solution. This solution relies solely on mathematics and open-source code, ensuring a decentralized network with no additional trust assumption. It achieves cost-effective scaling as user activity grows and provides a seamless user experience with one-click swaps, gas-less in-layer transactions, and instant LP exit. This makes OpenBit a promising solution for secure and efficient blockchain bridging.

Our decision was guided by a thorough evaluation of each solution's technical merits and their alignment with our objectives for security, decentralization, and scalability in bridging within the Bitcoin ecosystem.

B. *Functional Architecture as a Bitcoin liquidity market*

As previously discussed, one of the significant challenges in the Bitcoin ecosystem is the liquidity problem. In our evaluation of different solutions to address this issue, we have considered their strengths and limitations:

- Bitcoin scaling solutions employ various mechanisms to tackle scalability and/or programmability issues. These mechanisms include the Bitcoin-rooted Lightning Network, rollup-based Layer 2 solutions, sidechain-based Layer 2 solutions, or MSG-based Layer 2 solutions. While each solution has its unique strengths in expanding Bitcoin's scale and balancing the trade-off between scalability and security, they do not directly address the liquidity problem. Bitcoin scaling solutions primarily focus on enhancing scalability and transaction throughput within the Bitcoin ecosystem. However, they typically only support bridging or transferring Bitcoin assets from Bitcoin layer 1 to layer 2, without facilitating bridging into other blockchains. This limitation means that Bitcoin assets remain confined within the Bitcoin system, hindering access to new users and capital from outside the ecosystem and perpetuating the liquidity shortfall.
- Bridges that support Bitcoin assets have the potential to facilitate cross-chain liquidity by employing various technical solutions to be compatible with both Bitcoin and other blockchains. These solutions include PoS-based bridges, MPC-based bridges, and side-chain-based bridges. While these bridges can effectively bridge Bitcoin assets into other blockchains, their functionality is often limited. Typically, these projects primarily focus on the bridging aspect and may lack the capability to handle additional demands such as asset swapping, lending, staking, or other DeFi operations. These additional functionalities are crucial for providing deeper liquidity to assets and unlocking their full value within the broader blockchain ecosystem. Therefore, while bridges can address the immediate need for cross-chain asset transfer, further enhancements are necessary to fully address the liquidity problem and realize the potential of Bitcoin assets in decentralized finance.
- Centralized exchanges offer an alternative solution to address liquidity problems in the Bitcoin ecosystem. They provide a wide array of toolkits and support various financial operations such as investment, lending, and options trading. This broad functionality significantly lowers the barriers to entry and provides options for users who may not have direct access to trade Bitcoin assets. However, centralized exchanges also come with several limitations. Firstly, while many of them support Bitcoin (BTC), they may not support other assets like BRC-20 tokens or other innovative assets, limiting the diversity of trading options available to users. Secondly, as their name suggests, centralized exchanges operate on a centralized model, which contradicts the decentralized ethos of Bitcoin. The security of these exchanges relies on trust in a centralized commercial entity, exposing users to risks such as regulatory challenges and governance issues within the company itself.

Therefore, we propose OpenBit, a dedicated liquidity layer designed specifically to address the liquidity problem within the Bitcoin ecosystem. It combines the advantages of Bitcoin scaling solutions while maintaining the robust security of Bitcoin through its reward-penalty mechanism and the design of its TEE network. Additionally, OpenBit incorporates the flexibility of bridges, enabling seamless cross-chain transactions. Furthermore, it offers the functionality of centralized exchanges, supporting various DeFi operations such as asset swapping, staking, lending, and more.

OpenBit is not merely a Bitcoin layer 2 solution, a bridge, or a centralized exchange. Instead, it serves as a unique and comprehensive infrastructure solution that fills a significant gap in the industry ecosystem. By integrating the strengths of various approaches and technologies, OpenBit provides a holistic solution to the liquidity challenges faced by the Bitcoin ecosystem, paving the way for enhanced usability, accessibility, and efficiency in decentralized finance.

VIII. User Journey

A. *Preparation*

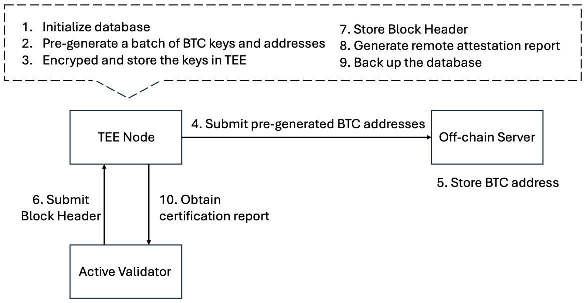

1. Initialize database
2. Pre-generate a batch of BTC keys and addresses
3. Encryped and store the keys in TEE
7. Store Block Header
8. Generate remote attestation report
9. Back up the database
TEE Node
4. Submit pre-generated BTC addresses
Off-chain Server
5. Store BTC address
6. Submit Block Header
10. Obtain certification report
Active Validator

Figure 6. Preparation

The TEE nodes initialize a batch of user Bitcoin keys and addresses, encrypting and storing them securely. These addresses are then submitted to the backend service for user registration. Meanwhile, the Active Validators submit verification data, such as Bitcoin block headers, to the TEE nodes, which verify and store this information. The TEE nodes subsequently generate a remote attestation report for the current environment and back up their database. Finally, the Active Validators retrieve and verify the remote attestation report from the TEE nodes, ensuring its integrity for presentation to users.

B. Deposit

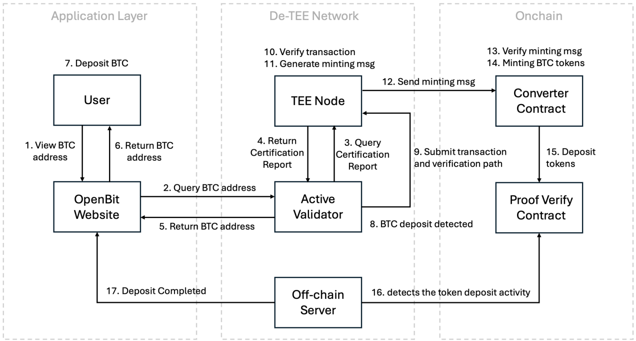


Figure 7. Deposit

Upon visiting the website, users can view their Bitcoin deposit address. The website retrieves this address through Active Validators, which obtains attestation reports from the TEE nodes. The TEE nodes thus return the attestation report containing environmental details and the deposit address. The Active Validators then verify the report's legitimacy and forward the address to the website for user access. Users proceed to deposit funds into the provided address. Subsequently, the Active Validators monitor the Bitcoin network, detect the deposit transaction, and relay both the transaction and its verification path to the TEE node. Using block headers, the TEE node validates the transaction and, upon successful verification, generates a corresponding minting message. This message is transmitted to the Ethereum conversion contract, where its legitimacy is confirmed, and BTC tokens are minted. The conversion contract then utilizes a proof verification contract to complete the token deposit. Meanwhile, OpenBit's backend service identifies and records the token deposit activity in its database. Once the deposit is confirmed, the backend service notifies the website, prompting user acknowledgment of the completed deposit.

C. Withdrawal

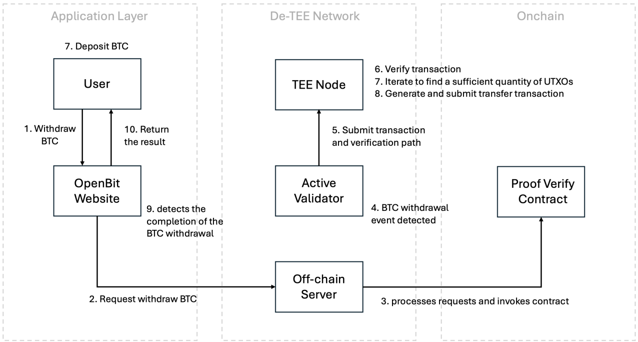

Application Layer
De-TEE Network
Onchain
7. Deposit BTC
User
TEE Node
6. Verify transaction
7. Iterate to find a sufficient quantity of UTXOs
8. Generate and submit transfer transaction
1. Withdraw BTC
10. Return the result
5. Submit transaction and verification path
OpenBit Website
9. detects the completion of the BTC withdrawal
Active Validator
4. BTC withdrawal event detected
Proof Verify Contract
Off-chain Server
2. Request withdraw BTC
3. processes requests and invokes contract

Figure 8. Withdrawal

The process begins as the user initiates a Bitcoin withdrawal request on the website, triggering a notification to the backend service. Subsequently, the backend service handles the request, ensuring its execution by submitting the transaction to the proof verification contract. Simultaneously, the Active Validators detect the Bitcoin withdrawal event and forward both the transaction and relevant verification paths to the TEE nodes. These TEE nodes then meticulously verify the transaction's legitimacy before proceeding to iteratively search for a sufficient quantity of UTXOs. Once the necessary UTXOs are found, the TEE nodes generate a transfer transaction, which is promptly submitted to the Bitcoin network. Upon completion of the BTC withdrawal, the website promptly detects the event and proceeds to notify the user, ensuring a seamless and efficient withdrawal process.

D. Forced Exit

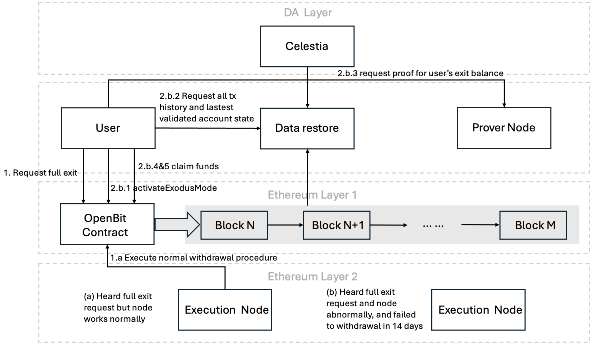

DA Layer
Celestia
2.b.3 request proof for user's exit balance
2.b.2 Request all tx history and lastest validated account state
User
Data restore
Prover Node
1. Request full exit
2.b.4&5 claim funds
2.b.1 activateExodusMode
Ethereum Layer 1
OpenBit Contract
Block N
Block N+1
... ...
Block M
1.a Execute normal withdrawal procedure
Ethereum Layer 2
(a) Heard full exit request but node works normally
Execution Node
(b) Heard full exit request and node abnormally, and failed to withdrawal in 14 days
Execution Node

Figure 9. Forced Exit

In the unlikely scenario that OpenBit service fails to work, we offer users a forced exit option to withdraw their tokens. A user may request a refund by calling requestFullExit in OpenBit contract. There can be two different cases after the requestFullExit invocation. If the Execution Layers successfully fulfill normal tasks within 14 days, users calling requestFullExit may get their tokens back through the normal withdrawal process described in the previous section. However, if Execution Layers fail to do so in the 14-day period starting from the requestFullExit invocation, OpenBit contracts enable users to freeze the contracts by calling activateExdusMode. In ExodusMode, all users can use Data Restore to retrieve their transaction history from OpenBit contracts calldata and DA layers as long as the latest account state is verified by Ethereum L1. Those data will be sent to the Prover Node in the De-TEE network, which will generate proofs. Users can thus call performExodus to get their tokens back once the proof of their account state is verified by the Verification Contract. If a user happens to deposit some tokens when the OpenBit contracts in ExodusMode, they can call cancelOutStandingDepositsForExodusMode to ensure a full refund.

IX. Security Analysis

In this section, we will formulate the protocol introduced in previous sections and conduct a security analysis.

Protocol 1 TEE Node Protocol

```
TEE Setup.
    Generate a set of Bitcoin addresses $Address$ and private keys $S_k$ pair
    Store encrypted $S_k$
    Send $Address$ to OpenBit frontend/backend
    Generate and store Ethereum key pair encrypted $sign_{sk}$ and $sign_{pk}$
    Publish $sign_{pk}$
    Contact k different Bitcoin and ETH nodes (including Active Validators) to get the latest block headers $BH$ and $EH$

procedure 1: KeyGeneration()
    Select one pre-generated address $Address$
    return $Address$
end procedure 1

procedure 2: DepositKeyControl($Tx$, $Address$, $To$)
    if verify($Tx$, $Address$) == True then
        set $mintTransaction.amount$ = $Tx.amount$
        set $mintTransaction.to$ = $To$
        sign $mintTransaction$ with $sign_{sk}$
        send $mintTransaction$
    end if
end procedure 2

procedure 3: WithdrawKeyControl($Tx$,$Address$)
    if verify $Tx$ == True then
        make $UTXO$ with $UTXO.amount$ = $Tx.amount$
        sign $UTXO$ with $S_k$ and send $UTXO$ to $Address$
    end if
end procedure 3
```

Note that all procedures and the set in Protocol 1 run in TEE enclave provided by specified TEE vendors (Intel SGXArm TrustZoneAWS Nitr etc.). The TEE setup procedure will prepare all ingredients and prepare remote attestation for verification.

If a deposit request is received, the De-TEE network would first call KeyGeneration() to get a new deposit address and actively listen and wait for the deposit to happen. Then, it would call DepositKeyControl() with all needed transaction information, waiting for a signed $mintTransaction$ to send to Bridge Contract.

If a user wants to withdraw BTC, De-TEE network listens to Bridge Contract to emit a burn event. A burn event will be emitted only if the Verification Contract can verify the ZKP of such burning operations. Then it will call WithdrawKeyControl() with all transaction information, which would sign and send the UTXO to the user's wallet

We also present the details of protocol 2, which also runs in the De-TEE network, which reflects the protocol described above

Protocol 2 Bridge Protocol

```
procedure 1: DepositHandler()
    // Once receive deposit request,
    Call $address$ = KeyGeneration()
    // Activate Validators keep listening to Bitcoin, once a deposit event happens and is verified,
    Call $mintMessage$ = DepositKeyControl($Tx$, $Address$)
    Send $mintMessage$ to Bridge Contract
end procedure

procedure 2: WithdrawHandler()
    // Once receive withdraw request,
    // Activate Validators keep listening to Ethereum, once a verified burn event happens,
    Extract transaction information $Tx$ and $Address$
    Call WithdrawKeyControl($Tx$, $Address$)
    // It will send desired UTXO to the user's withdrawal wallet
end procedure
```

We show that our protocols' security satisfies consistency and liveness properties in the following theorem.

Theorem 1. *system implemented by De-TEE Network Protocol and Bridge Protocol satisfies consistency and liveness properties under the assumptions that*

1) *For each component of the De-TEE network, at least one honest node is alive.*
2) *Both Bitcoin and Ethereum are consistent (verified transaction must have happened) and live (a valid transaction will always go through)*
3) *zk-proof system implemented satisfies both completion and soundness properties*
4) *Attackers have bounded computing power*

Proof. First, the liveness property follows the liveness assumption of the De-TEE netowrk and both Bitcoin and Ethereum.

Then we will show the consistency property. In the deposit direction, by assumption 1, there is at least one honest Active Validator node, which listens and reads Bitcoin transactions, which will be consistent with the Bitcoin blockchain, the depositKeyControl() will only be invoked after a deposit transaction confirmed happens, which will further sign and send $mintTransaction$ specifying the amount of BTC in deposit address. On Ethereum, the Bridge contract will mint an equal amount of tokens if and only if it receives a valid signed $mintTransaction$, which may not be faked by an adversary with bounded computing power, as stated in assumption 4. Thus the whole deposit operation will preserve consistency between Bitcoin and Ethereum. In the withdrawal direction, a burn event will be emitted if and only if zk-proof is generated and verified. This is a consistent operation by assumption 3. By assumption 1, at least one of the honest Active Validators will capture the event emitted and send the transaction details including the amount of tokens burned to the TEE enclave, which will further unlock the exact amount of BTC in the deposit address and send them to the user's wallet. Hence a withdrawal operation will preserve consistency between Ethereum and Bitcoin. And thus we complete our proof. □

X. Conclusion

In conclusion, OpenBit emerges as a groundbreaking solution to the liquidity challenges plaguing the Bitcoin ecosystem. By leveraging cutting-edge cryptographic technologies, OpenBit offers a secure, efficient, and decentralized cross-chain liquidity layer. Through its innovative De-TEE network, OpenBit ensures the integrity and reliability of asset transfers across multiple blockchain networks, unlocking new opportunities for BTC holders and developers alike. With its modular architecture, OpenBit presents a flexible and scalable solution capable of accommodating diverse use cases and future advancements within the Bitcoin ecosystem. As Bitcoin continues to evolve, OpenBit stands ready to facilitate its integration with other blockchain networks, driving innovation and growth in the decentralized finance landscape.

XI. Appendix 1: Further Discussion on OpenBit Bridge

One of the core features of our product is the cross-chain bridge, designed to enhance Bitcoin liquidity by connecting it with vibrant ecosystems across various blockchains. In this section, we'll explore existing Bitcoin cross-chain bridge solutions and evaluate their respective merits and drawbacks.

A. Classification of Existing Cross-Chain Bridges

1) Classification based on Supported Message Types: **Arbitrary Message Bridge (AMB)**: A bridge enables the transfer of various message types, facilitating complex functionalities such as cross-chain contract invocations and computations.

Wrap Bridge: A bridge can facilitate transfers by allowing the asset to be "wrapped" in a form that can be recognized and transferred between the two networks.

Swap Bridge: A bridge enables exchanging tokens within the pool, effectively swapping asset's native form for another asset in the target chain.

In most industrial applications, AMB usually serves as the underlying support for Wrap Bridge and Swap Bridge. In a sense, Swap and Wrap bridges are one of the applications built on top of AMB.

2) Classification based on the verification methods: **Native Verification**: involves deploying a lightweight node of the source chain on the target chain to verify messages sent from the source chain. The process includes introducing a Head Relayer network responsible for relaying block headers from the source chain to the target chain. Subsequently, the lightweight node program on the target chain verifies the block headers provided by the Head Relayer.

Local Verification: Involves peer-to-peer verification, where transaction counterparts directly verify transactions. The typical paradigm is atomic swaps based on hash time locks, where parties verify each other's actions. In practice, most cross-chain projects with local verification use an intermediary liquidity provider as a public transaction counterpart.

External Verification: Involves introducing a group of external witnesses to verify cross-chain information. Users must trust these witnesses, who may depend on mechanisms like MPC networks, POS networks, TEE networks, multisignature groups, or Oracles to achieve consensus.

Native verification entails minimal trust assumptions. However, seamlessly deploying Bitcoin's light nodes into other mature chains is challenging due to the current multi-chain ecosystem. On the other hand, local verification requires no trust assumptions and is adaptable to multiple chains but is limited in scope, supporting only Swap Bridge. The majority of active projects in the market rely on solutions based on external assumptions, making this classification a focal point of our subsequent discussion.

B. Bitcoin Cross-Chain Bridges in the Market

We've conducted research on nearly 10 cross-chain projects with financing records over the past three years. Most of them have been in the seed and Series A funding rounds, typically raising funds in the range of millions of dollars. However, there are also standout projects like Polyhedra and Cobo that have progressed to Series B and beyond, accumulating total funding amounts exceeding \$20 million. In this section, we will examine how each project implements cross-chain transactions of Bitcoin assets onto other chains from a technical standpoint.

The Pos-based Bridge approach, exemplified by Polyhedra [16], THORCHAIN [17], relies on staking mechanisms and user-initiated reporting to ensure security. However, this requires validators to stake significant capital, incurring substantial costs and potentially leading to long waiting times for LP(Limited Partner) exit.

The MPC-based Bridge solutions, such as Cobo, are backed by various trusted parties, which carries the risk of centralization. Additionally, the computationally intensive MPC (Multi-Party Computation) process can lead to slower transaction speeds, and the higher costs associated with the infrastructure provider can further impact the user experience.

Sidechain-based mechanisms, like Liquid Network [12], leverage the reliability of the Bitcoin network for security but are limited to supporting only the Bitcoin and its sidechain pair, resulting in very slow performance that cannot be extended to other chains.

TEE-Based solutions, represented by Bool Network [21], face the risk of single-point failure from the TEE (Trusted Execution Environment) manufacturer and operator. The expenses linked to TEE hardware and configuration needs can be significant, and prolonged waiting periods for committee operations could also hurt user experience.

In contrast, the De-Tee Network-based OpenBit relies solely on math and open-source code, ensuring a decentralized network immune to single-point failures. It achieves cost-effective scaling as user activity grows and provides a seamless user experience with one-click swaps, gas-less in-layer transactions, and instant LP exit. This makes OpenBit a promising solution for secure and efficient blockchain bridging.

XII. Appendix 2: How OpenBit Works with Partners

A. *Enhancing Bitcoin Asset Ecosystem*

The Bitcoin Asset Offering Protocol witnessed significant growth in Q1 2023, with the market booming by Q4. Within the Ordinals protocol ecosystem [9], various tokens like BRC20 [22] led to a noticeable wealth effect. Over time, prominent protocols emerged, such as Ordinals [9], Atomicals [23], Taproot Assets [7] [8], Runes [9], and PIPE. Among these assets, OpenBit already supports BTC and BRC-20-related assets for bridging and swapping. Moving forward, we aim to expand its support to a broader range of assets.

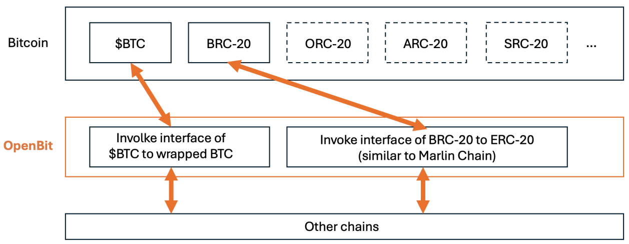


Figure 10. Technical Integration Between OpenBit and BTC Assets

B. *Empowering Bitcoin Layer 2*

Scalability remains a significant concern for Bitcoin due to inherent design limitations, such as its 1 MB block size, 10-minute block generation time, and bandwidth constraints. Following key technological upgrades like Segwit [5] and Taproot [7] [8], many developers are now turning to layer 2 solutions to mitigate these challenges.

The evolution of Bitcoin Layer 2 solutions has progressed from Lightning Network (LN) [10], leveraging Bitcoin's native mechanisms for rapid micropayments, to considerations of sidechain solutions like Rootstock (RSK) [14]. More recently, the focus has shifted towards rollup solutions such as B2 Network [24] and BitVM [25], based on zkRollup and optimistic rollup respectively, offering promising avenues for scalability and efficiency improvements.

OpenBit primarily concentrates on EVM-compatible Layer 2 solutions, allowing for easy bridging and cross-chain asset swapping, thereby enhancing liquidity.

1) Bitcoin-Rooted Layer 2: Lightning Network

When discussing Bitcoin layer 2 solutions, the most renowned one is the Lightning Network [10]. Originally designed to facilitate fast and low-cost micropayments, the Lightning Network operates through two-party, multisignature ”channels” in Bitcoin addresses. These channels are represented as entries on the Bitcoin public ledger. To spend funds from a channel, both parties must agree on the new balance, which is stored as the latest transaction signed by both. To initiate a payment, both parties sign a new exit transaction spending from the channel address, thereby invalidating all previous exit transactions.

2) Rollup-based Layer 2: Rollup-based Layer 2 solutions aim to alleviate congestion on Layer 1 by moving multiple transactions onto a separate network, where they are consolidated into a single data package. This package is then transmitted back to Layer 1 for inclusion. In recent times, numerous new projects have emerged, primarily focusing on two directions: zero-knowledge rollup and optimism rollup.

- zkRollup Layer 2: B2 network [24], Merlin Chain [26]
  zkRollup, represented by projects like B2 Network and Merlin Chain, fundamentally operates by completing transactions on a layer 2 network. All transaction activities are recorded on a rollup, where multiple transactions are aggregated to generate a zero-knowledge proof (ZKP). This ZKP is then written into the Bitcoin inscription.

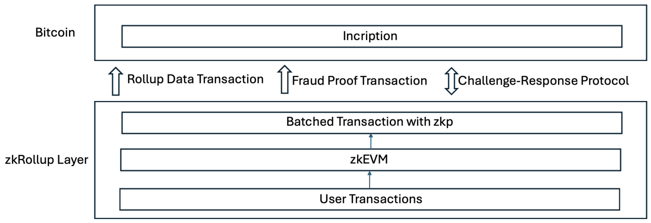


Figure 11. zkRollup architecture

- opRollup Layer 2: BitVM [25]
  In opRollup, represented by projects like BitVM, the complete process involves compiling the program into a large binary circuit by the prover and verifier. The prover commits the program to a Taproot address bit by bit, which contains a leaf script for each logic gate in the circuit. Subsequently, the pre-signed series of transactions between them support verification and challenge using opcodes. If the prover submits an incorrect claim, the verifier has the authority to seize their deposit.

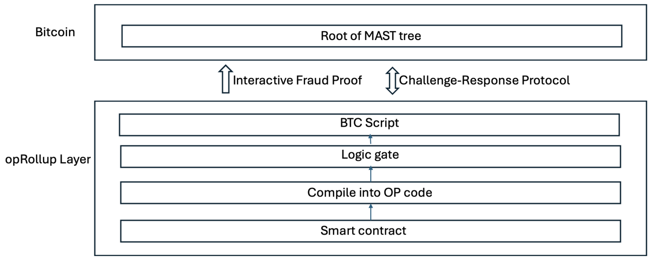


Figure 12. opRollup architecture

3) Sidechain-based Layer 2: Rootstock [14], Stacks [11], Liquid [12]

Sidechain-based Layer 2 solutions, exemplified by projects like Rootstock (RSK), Liquid, Stacks, and BEVM [15], offer innovative approaches to enhance the functionalities of the Bitcoin network. These solutions enable interoperability and scalability by allowing for the concurrent processing of Bitcoin and sidechain transactions. For instance, Rootstock enables Bitcoin miners to process both BTC and RSK transactions concurrently, expanding Bitcoin's functionality with EVM support. Liquid facilitates the movement of Bitcoin between networks using a two-way peg, albeit with centralized control, while Stacks incentivizes stakers to pledge STX and earn BTC rewards.

4) MSG-based Layer 2: Mirror [27]

Mirror starts by implementing a multi-signature node mechanism, employing a Multi-Signature Group (MSG) algorithm. The principle involves dividing hundreds to thousands of nodes into groups, where each node can be paired with any other four nodes. Each group consists of five nodes, and any three nodes within the group can execute multi-signature transactions for the assets within the group. Additionally, each node is required to stake 1 mBTC in a designated smart contract, with the risk of forfeiting the stake in case of malicious behavior. For instance, with 1000 nodes, approximately 3000 groups can be generated. If each node stakes 1000 BTC, each group can hold 1 BTC. In the event of malicious intent from a node, at least three nodes in any group must collectively engage in malicious behavior, and they must also forfeit 3 mBTC.

While the architectures of various layer 2 solutions differ significantly, OpenBit provides a universal protocol compatible with their incentive assets. These assets include tBTC from the B^2 network, sBTC from Stacks, mBTC from Mirror, and others.

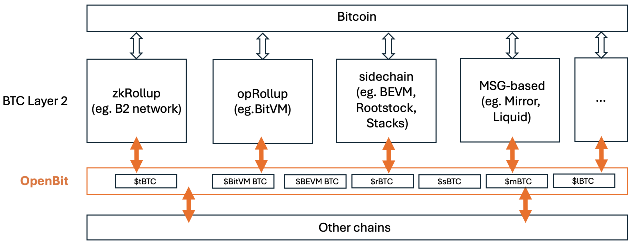


Figure 13. Technical Integration Between OpenBit and Bitcoin Layer 2

OpenBit provides a standardized interface for EVM-compatible layer 2 solutions, facilitating seamless integration of assets. These assets can subsequently be leveraged across OpenBit's ecosystem for a myriad of DeFi protocols and tools.

C. Enriching Bitcoin restaking chain, Ethereum and other chains

OpenBit will facilitate the seamless transfer of various asset forms into the ones compatible with target chains, breaking down barriers between different chains and significantly enhancing liquidity levels.

For instance, consider restaking chains like Babylon and BounceBit, which are prominent in the Bitcoin ecosystem.

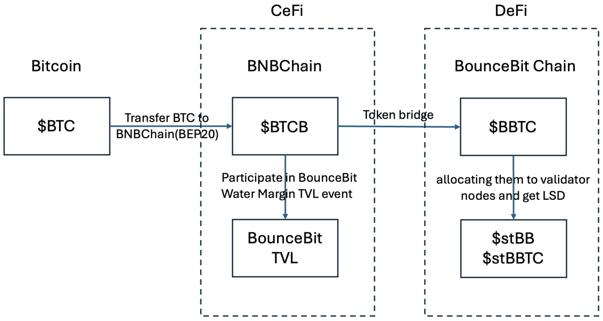

CeFi
DeFi
Bitcoin
BNBChain
BounceBit Chain
$BTC
Transfer BTC to BNBChain(BEP20)
$BTCB
Token bridge
$BBTC
Participate in BounceBit Water Margin TVL event
BounceBit TVL
allocating them to validator nodes and get LSD
$stBB
$stBBTC

Figure 14. BounceBit mechenism

1) CeFi-based Restaking Chains: BounceBit

BounceBit utilizes centralized finance (CeFi) for secure staking, employing a straightforward mechanism: Start by transferring your BTC to Binance exchange's BNBChain (BEP20), where it is automatically converted into BTCB (Wrapped Bitcoin on the BNB Chain). Then, deposit your BTCB on the BounceBit Water Margin TVL event page or bridge your BBTC to BounceBit's Layer 1, integrating them into the broader BounceBit ecosystem simultaneously.

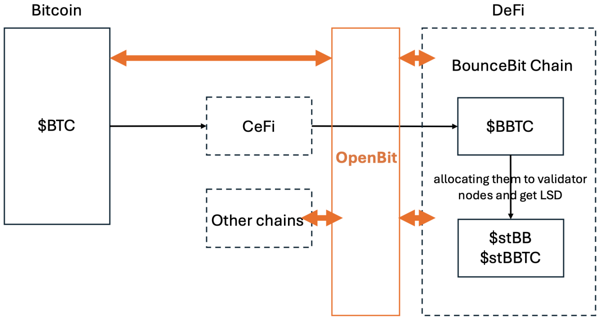


Figure 15. Technical Integration Between OpenBit and BounceBit

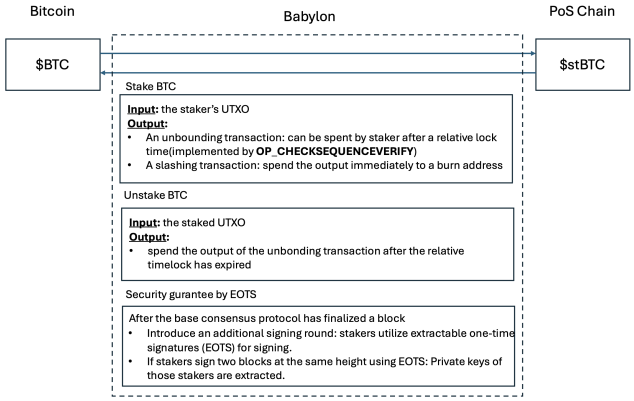
For CeFi-based restaking chains like BounceBit, OpenBit serves as a gateway with two collaboration options:

1. Facilitating the direct bridging of Bitcoin assets into the BounceBit chain, offering a more streamlined bridge service akin to centralized exchanges. This approach leverages Trusted Execution Environments (TEE) and zero-knowledge proofs (ZKP) to ensure security.

2. Acting as a frontend to bridge assets from other chains, enabling asset swapping into formats accepted by the BounceBit chain, such as BBTC.

We believe these collaborative approaches will undoubtedly offer several benefits for BounceBit, including an expanded asset range and enhanced liquidity. OpenBit, acting as a traffic gateway, can introduce more new users and new staking assets to BounceBit, thereby boosting its growth and ecosystem development.

2) DeFi-based Restaking Chains: Babylon [28]



Stake BTC

Input: the staker's UTXO
Output:

- An unbounding transaction: can be spent by staker after a relative lock time(implemented by **OP_CHECKSEQUENCEVERIFY**)
- A slashing transaction: spend the output immediately to a burn address

Unstake BTC

Input: the staked UTXO
Output:

- spend the output of the unbonding transaction after the relative timelock has expired

Security gurantee by EOTS

After the base consensus protocol has finalized a block

- Introduce an additional signing round: stakers utilize extractable one-time signatures (EOTS) for signing.
- If stakers sign two blocks at the same height using EOTS: Private keys of those stakers are extracted.

Figure 16. Babylon mechenism

Unlike BounceBit, DeFi-based restaking projects like Babylon primarily focus on innovating on the original Bitcoin script to achieve decentralized staking. The core infrastructure of Babylon is a Bitcoin staking protocol that acts as a control plane between Bitcoin and PoS chains.

Specifically, Babylon protocol relies on two key technological components:

1. Staking Contracts via Bitcoin Covenant Emulation: Staking contracts on Bitcoin are expressed through UTXO transactions using Bitcoin script. These contracts involve staking, unbonding, slashing, and unstaking transactions, leveraging Bitcoin covenants to constrain transaction outputs.

2. Automated Slashing via Accountable Assertions and Finality Gadgets: To address safety violations, the protocol utilizes accountable assertions and finality gadgets. It employs extractable one-time signatures (EOTS) in an additional signing round after block finalization to ensure block security. In the event of safety breaches, the private keys of offending stakers can be extracted, allowing for slashing transactions.

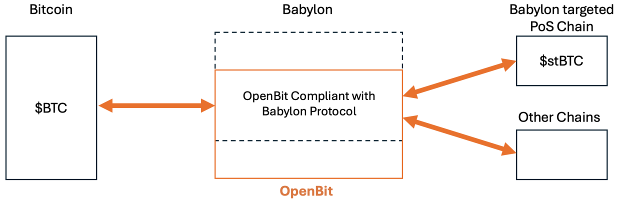

Bitcoin
Babylon
Babylon targeted PoS Chain
$BTC
OpenBit Compliant with Babylon Protocol
$stBTC
Other Chains
OpenBit

Figure 17. Technical Integration Between OpenBit and Babylon

OpenBit seamlessly integrates with the Babylon protocol, ensuring security while facilitating ecosystem sharing. This integration provides users participating in Babylon's Bitcoin staking with enhanced liquidity and a broader array of DeFi options.

References

[1] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008

[2] Vitalik Buterin. *A next-generation smart contract and decentralized application platform*, 2014.

[3] Anatoly Yakovenko. *Solana: A new architecture for a high performance blockchain v0. 8.13*, 2018.

[4] Kevin Sekniqi, Daniel Laine, Stephen Buttolph, and E Gu n Sirer. *Avalanche Platform*, 2020.

[5] Eric Lombrozo, Johnson Lau, and Pieter Wuille. *Segregated Witness (Consensus layer)*, 2015.

[6] Pieter Wuille, Jonas Nick, and Tim Ruffing. *Schnorr Signatures for secp256k1*, 2020.

[7] Pieter Wuille, Jonas Nick, and Anthony Towns. *Taproot: SegWit version 1 spending rules*, 2020.

[8] Pieter Wuille, Jonas Nick, and Anthony Towns. *Validation of Taproot Scripts*, 2020.

[9] Casey Rodarmor. *Ordinary Theory Handbook*, 2023.

[10] Joseph Poon and Thaddeus Dryja. *The bitcoin lightning network: Scalable off-chain instant payments*, 2016.

[11] Stacks Network. *Stacks: A Bitcoin Layer for Smart Contracts*. 2022.

[12] Jonas Nick, Andrew Poelstra, and Gregory Sanders. *Liquid: A bitcoin sidechain*. 2020.

[13] Maxim Orlovsky, Peter Todd, Giacomo Zucco, Federico Tenga, and Olga Ukolova. *RGB Blackpaper: Turing-complete, Scalable Confidential Smart Contract Layer for Bitcoin LN*. 2015.

[14] SD Lerner. *Rootstock platform, bitcoin powered smart contracts*, 2020.

[15] BEVM Foundation. *BEVM: An EVM-compatible Bitcoin Layer 2 with BTC as gas*, 2023

[16] Xie, Tiancheng and Zhang, Jiaheng and Cheng, Zerui and Zhang, Fan and Zhang, Yupeng and Jia, Yongzheng and Boneh, Dan and Song, Dawn. *zkBridge: Trustless Cross-chain Bridges Made Practical*, 2022

[17] THORChain, *THORChain: A Decentralised Liquidity Network*, 2020

[18] Sabt, Mohamed and Achemlal, Mohammed and Bouabdallah, Abdelmadjid, *Trusted execution environment: What it is, and what it is not*, 2015

[19] Fiege, Uriel and Fiat, Amos and Shamir, Adi, *Zero knowledge proofs of identity*, 1987

[20] Gabizon, Ariel and Williamson, Zachary J and Ciobotaru, Oana, *Plonk: Permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge*, 2019

[21] Zeyuan Yin, Bingsheng Zhang, Jingzhong Xu, Kaiyu Lu, and Kui Ren. Bool network: An open, distributed, secure cross-chain notary platform, 2022.

[22] Taproot Wiz, Va Mo, Conrad Mo, *BRC Standard: the BRC20 Ordinals yield-bearing index protocol*, 2023

[23] Atomicals Protocol, *Atomicals Guidebook*, 2024

[24] B^2 Team, *B^2: THE MOST PRACTICAL BITCOIN LAYER-2 NETWORK*, 2024

[25] Robin Linus. *BitVM: Compute Anything on Bitcoin*. 2023.

[26] Eason.Z, Rilke, shier, Hannah, *Merlin Bridge WhitePaper*, 2024

[27] Mirror Team, *The Mirror Protocol White Paper*, 2021

[28] Ertem Nusret Tas, David Tse, Fisher Yu, Sreeram Kannan, *Babylon: Reusing Bitcoin Mining to Enhance Proof-of-Stake Security*, 2022