Cointelegraph Research

PORTAL TO BITCOIN

HOW PORTAL TO BITCOIN SOLVES CROSS-CHAIN LIQUIDITY CHALLENGES







Cointelegraph Research Report

Content

1. The Future of Bitcoin-centric DeFi 3

2. Overview and Comparison of Cross-chain Bridging Technologies 6

2.1 Price oracles 7

2.2 Cross-Chain Interoperability Protocols 8

2.3 Threshold Cryptography bridges 12

2.4 Portal to Bitcoin 9

Introducing BitScaler: Scaling Bitcoin for DeFi and Beyond 13

- What is BitScaler? 13
- Customized Channel Factories 14
- Benefits 15
- Policy Scripts and Miniscript 15
- Solving the AMM Challenge on Bitcoin 15
- How BitScaler Solves the Automated Market Makers (AMMs) Implementation 15
- Atomic swaps using the AMM 16
- Hook and Allocation Transactions in Detail 16
- Trader and Liquidity Provider Channels 17
- Non-Custodial Delegation 17

2.4.1 Portal's Automated Dynamic Market Maker (ADMM) 22

2.4.2 Portal DeFi's Tokenomics and Network Incentives 24

3. Conclusion 25

Disclaimer 26

1. The Future of Bitcoin-centric DeFi

While Bitcoin's success as a digital store of value is undeniable, its current utility beyond storage and transfer has remained limited. It is particularly limited when it comes to integrating with DeFi applications available on Turing complete smart contract blockchains due to cross-chain custody risk.

It is mostly seen as an unproductive asset and relies heavily on custodial, exogenous infrastructure to trade and lend against.

However, recent technical advancements have spurred a flurry of new developer activity in the Bitcoin L2 ecosystem. This is likely to lead to an explosion of Bitcoin-native DeFi in the coming years. Ethereum currently dominates the DeFi space and holds approximately $48 billion of the total TVL across all blockchains as of August 2024.

Bitcoin's DeFi TVL is at ~$1.9 billion [1] at the time of writing, with the largest sidechain being Bitlayer at $358m and the two largest protocols being BitFi and AILayer at $244 million and $126 million, respectively. If Bitcoin were to capture just 10% of Ethereum's DeFi market, it could gain over $4.8 billion in TVL.

Arguably, this number could be even higher because Ethereum fails to successfully serve one of the most sought-after use cases in crypto lending against a Bitcoin stash.

Currently, the only liquidly traded wrapped Bitcoin token on Ethereum is WBTC. WBTC not only introduces counterparty risk and trust but swapping with BTC results in a fee of 1-2% through most CEXs and bridges (except for ThorChain).

When taking out a low-TVL loan against large Bitcoin holdings, swap fees alone could thus easily match or outweigh the interest expense — an unacceptable cost to most users.

The absence of Bitcoin-native DeFi to serve this demand for BTC-derived financial products can be attributed to the technical limitations of Bitcoin's base layer. Because it prioritizes robustness, decentralization and security, Bitcoin only processes seven simple transactions per second, which is insufficient to handle the throughput of many DeFi applications.

Bitcoin also has much less scripting capabilities than other chains. While modern smart contract blockchains allow developers to store information onchain that can later be accessed through function calls, Bitcoin script is stateless. It is only used to set the conditions to unlock a UTXO for spending, and it does so using a simple stack-based machine with very few OP codes.

[1] Note: This figure represents the aggregate total derived from the TVL of Bitcoin's mainchain and sidechains, as reported by DeFiLlama. Accurate as of 8/22/24

This makes implementing liquidity pools, oracles or voting mechanisms infeasible.

In contrast, smart contract chains compile into Turing-complete VMs that can perform general computation.

To address the scalability limitations of the Bitcoin network and make scripting in the ecosystem more expressive, developers have proposed and built various scaling solutions and extensions to the base layer.

State channel networks

State channels are two-party onchain vaults. The participants of a channel can transact offchain by exchanging cryptographic commitments. This happens in a way that allows them to unilaterally withdraw their correct balance from the vault if desired. The Lightning Network and the Mercury Layer are Bitcoin L2 technologies constructed using such state channels.

Once on the mainnet, Mercury Layer will employ so-called state chains, based on a key-sharing mechanism, to enable offchain UTXO transfers. On the other hand, Lightning uses a routing mechanism to create a network from two-party payment channels.

Client-Side Verification

Client-Side Verification (CSV) is a technique for asset issuance in which transaction history is fully stored on the asset holder's hardware, and transactions are validated locally. Bitcoin's L1, is only used to post compact commitments as a double-spend protection.

With client-side validation, transaction details remain private and visible only to the involved parties. CSV L2 solutions include the RGB Protocol, Taproot Assets (formerly Taro), Bool Network, Bitmask, and Bitlight Labs.

Rollups

Rollups are a type of L2 that serves as an execution layer that interacts with the Bitcoin network for consensus. They bundle and execute multiple transactions offchain and post a succinct summary on the main chain.

Rollups can be grouped into two types: optimistic and ZK-rollups. Optimistic rollups such as Rollux and Rollkit assume that the posted summary is correct by default and only require proof to challenge a fraudulent submission.

In contrast, ZK-rollups use zero-knowledge proofs to verify the validity of all transactions within a batch. The B² Network and Satoshi VM are some of the Bitcoin projects exploring the application of ZK-rollups.

The need for bridges in a future L2 ecosystem

While all these solutions include some way of pegging BTC in and out of the base chain, this ability does not extend assets issued on the L2. The peg-out process will also incur significant costs during future fee spikes on the Bitcoin mainnet.

This will make the L2 ecosystem susceptible to the same liquidity fragmentation that currently besets L2 Ethereum. Solving this will require bridging mechanisms that integrate different Bitcoin scaling solutions horizontally without going through the base layer.

In this report, we explore some cross-chain technologies and protocols essential for blockchain interoperability. Each offers a distinct approach to cross-chain interoperability, but all projects share a common goal of facilitating seamless interactions between disparate blockchain environments. They have chosen different trade-offs between security, decentralization, and efficiency.

The report begins with how oracles verify and transmit real-world data to blockchains to ensure accurate price feeds for cross-chain swaps. We then discuss Chainlink's CCIP, a protocol to transfer tokens and data across blockchains.

Next, the report delves into Threshold Network's use of threshold cryptography for bridging assets as well as LayerZero, which enables flexible cross-chain messaging with its modular components.

Finally, we examine Portal to Bitcoin, a bridgeless protocol that simplifies cross-chain Bitcoin swaps using BitScaler, the first implementation of a modified channel factory, multiparty Hash Time Lock Contracts (MP-HTLCs) and a Multi-Chain layer 2 Automated Market Maker (MC-LAMM).

We cover how Portal's notary chain architecture and validator incentives ensure secure and trust-minimized cross-chain asset swaps while maintaining user control over assets.

By removing the need for wrapped tokens or custodial intermediaries, Portal to Bitcoin directly addresses the core issues of security, trust, and liquidity that have plagued other protocols, making it a critical solution for Bitcoin interoperability and cross-chain DeFi.

2. Overview and Comparison of Cross-chain Bridging Technologies

Table 1: Comparisons Of Cross-Chain Bridging Technology

Technology	Counterparty Risk	Decentralization	Trusted elements
Oracle-Based Networks	High	Moderate	Oracles
Proof of Stake Bridges	Moderate	High	Validators
Cross-Chain Messaging Protocols	High	High	Network Participants
Portal DeFi	Low	High	No External Trust other than participating chains

Table 2: Comparisons Of The Security Mechanisms Of Cross-Chain Bridging Technology

	Security Mechanism
Oracle-Based Networks	Oracles
Proof of Stake Bridges	Validators
Cross-Chain Messaging Protocols	Relayers & Proofs
Portal DeFi	Atomic Swaps between AMMs on Multiple Chains

2.1 Price oracles

Oracles provide the decentralized price feeds essential to facilitating cross-chain swaps on DEXs. They ensure conversion rates, such as for a swap of TRX on Ethereum to USDT on BSC, accurately reflect true market values during transactions.

However, permissionless systems face inherent risks, such as Sybil attacks in which an adversary attempts to skew the oracle output by submitting false data through multiple aggregating nodes. The trustworthiness of the oracle's output hinges on the integrity of the participating nodes.

In the 2020 Harvest Finance attack, an oracle manipulation led to a $24 million loss. The hack occurred because the protocol's price oracle failed to detect manipulated asset values in Curve.fi's Y pool.

The attacker exploited this flaw by arbitraging large amounts of USDC and USDT to distort their prices. The oracle used these manipulated prices to calculate share values in Harvest's vaults, enabling the attacker to deposit funds at artificially low prices and withdraw them at higher prices.

The exploit succeeded because the oracle did not reject the manipulated data, leading to significant financial losses for the protocol. So, while the use of well-decentralized oracles mitigates some risks, it cannot fully eliminate the data manipulation or inaccuracies, particularly if the data sources themselves are compromised.

Oracles typically collect data from multiple independent sources, such as APIs or financial providers. Depending on the individual project, nodes perform offchain aggregation by using predefined algorithms such as computing the median value of the submissions or requiring a certain percentage of nodes to agree within a specified range.

Chainlink is a notable example, where each node queries data from several sources (e.g., ETH/USD prices), calculates a local median, and exchanges results through an encrypted peer-to-peer network. Agreement on accuracy is reached, and the protocol selects one node to generate a report with cryptographic signatures from a quorum, which is then ultimately submitted onchain. A smart contract verifies the signatures and updates the price feed.

This approach minimizes trust by ensuring that no single node determines the final value. However, they have the same Sybil, collusion, and other consensus issues as other non-proof-of-work consensus systems. Cryptographic proof of quorum agreement guarantees the integrity of the process, assuming that the inputs can be trusted, while offchain computation reduces gas costs, enabling frequent updates.

To incentivize honest behavior, nodes stake $link tokens as collateral. The staking smart contract can slash the stake of nodes that consistently deviate from the consensus while rewarding accurate reporters.

The system maintains decentralization by distributing data collection across independent nodes, and the onchain verification process ensures that the final output reflects a collective agreement, reinforcing the decentralized nature of the oracle network.

2.2 Cross-Chain Interoperability Protocols

Cross-chain interoperability refers to the ability of different blockchains to communicate and exchange information with each other. Interoperability protocols enable such communication by setting rules and standards for message exchange and providing a trust-minimized framework for triggering actions across chains.

A cross-chain message may contain instructions, function calls, or any arbitrary data that can be interpreted and acted upon by the receiving blockchain.

Various communication standards have been created in an attempt to introduce a common language that all blockchain protocols can use to interoperate. In this section, we will discuss Chainlink's CCIP and LayerZero to highlight the core underlying principles and use cases of cross-chain interoperability protocols.

Chainlink CCIP

Chainlink's Cross-Chain Interoperability Protocol (CCIP) is an open standard protocol that enables the secure transfer of tokens and data across different blockchain networks.

It relies on Chainlink's decentralized oracle networks (DONs) to secure communication between offchain
and onchain components.

The offchain components in CCIP include the oracle nodes that observe and validate crosschain transactions. They also include infrastructure used for data processing and aggregation that occurs before onchain submission. These offchain elements work in conjunction with onchain smart contracts to enable secure cross-chain operations.

Upon initiating a cross-chain message, the router of the sending party relays it to the destination chain via Chainlink's decentralized oracle networks (Figure 1). This relay process occurs through CCIP's consensus layer, which operates as follows:

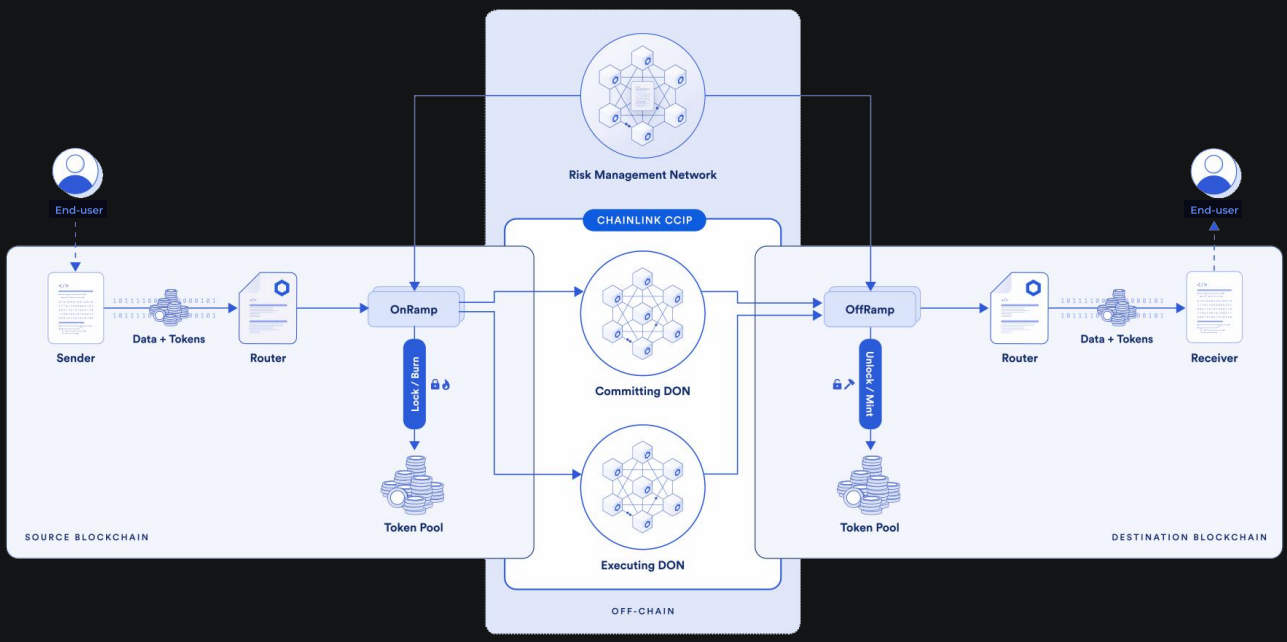
Nodes in the decentralized oracle network independently retrieve and validate the message data. They encrypt their observations using a threshold encryption scheme and forward them to a leader node. The leader node aggregates the encrypted data to determine the most common response and submits a cryptographically signed report onchain.

This aggregated message/data then passes through the committing DON for final validation while the active risk management network monitors the process for errors. To avoid single points of failure and make the final report tamper-resistant and verifiable, decryption of the consensus layer report requires a quorum of nodes.

Once validated, the executing DON translates the message/data into the destination chain's language and delivers it to the target blockchain.

The example below illustrates how CCIP facilitates secure cross-chain transactions.

Figure 1: Architectural Overview Of Chainlink's CCIP



Source: Chainlink

During the message transfer process, CCIP uses OCR 2.0 to ensure that only accurate transaction data from the committing chain is aggregated. Through comparison, the nodes reach an agreement on the most accurate data point, which is then submitted to the blockchain.

By processing and agreeing on data offchain before final submission, OCR 2.0 reduces gas costs. The system only needs to make a single onchain transaction with the aggregated result rather than multiple transactions from individual nodes.

To further ensure the system's security, CCIP implements rate limits on token transfers and controls the maximum capacity and refill rate for token transfers. This ensures that the system can handle the load without compromising security.

CCIP is deployed on 14 blockchain networks, including BSC, Ethereum, Base, and Polygon. Unlike traditional oracles, which that just primarily bring offchain data to onchain environments, CCIP enables a wide range of applications, such as token transfers, cross-chain smart contract calls, and data sharing. Projects that use CCIP include Sushi, ChainGPT, Micro3, ChainSwap, and SWIFT.

Other protocols offering Oracle-based cross-chain functionality are:

- **Cosmos:** Employs the Inter-Blockchain Communication (IBC) protocol to facilitate communication and token transfers between independent blockchains within the Cosmos ecosystem.
- **Band Protocol:** A network that provides secure and scalable cross-chain data oracles and provides reliable data feeds for various blockchains.
- **API3:** Offers decentralized oracle services that allow smart contracts to access real-world data through a network of decentralized APIs and supports cross-chain interactions.

LayerZero

LayerZero is another popular cross-chain interoperability protocol. In LayerZero's architecture, endpoints manage message traffic to and from blockchains, executors handle transmission, and DVNs verify the integrity of messages.

The entire structure maintains composability through the MessageLib Registry.

The cross-chain transmission of a message begins with Endpoints, which are nodes that interface with contracts deployed on each participating blockchain (Figure 2). These Endpoints handle the sending, verification, and receipt of messages and maintain a continuous connection with other Endpoints across the network.

Upon initiating a cross-chain transfer, a message is sent from the source blockchain's Endpoint and is then transmitted by LayerZero's Relayer to the Executor smart contract to be executed on the destination chain. Executors are pre-deployed contracts that process incoming messages to ensure efficient and timely delivery.

Before the message can be transmitted to its destination, its integrity must be confirmed. This is where Decentralized Verification Networks (DVNs) come into play. DVNs consist of independent validators who verify the payload hash of each message.

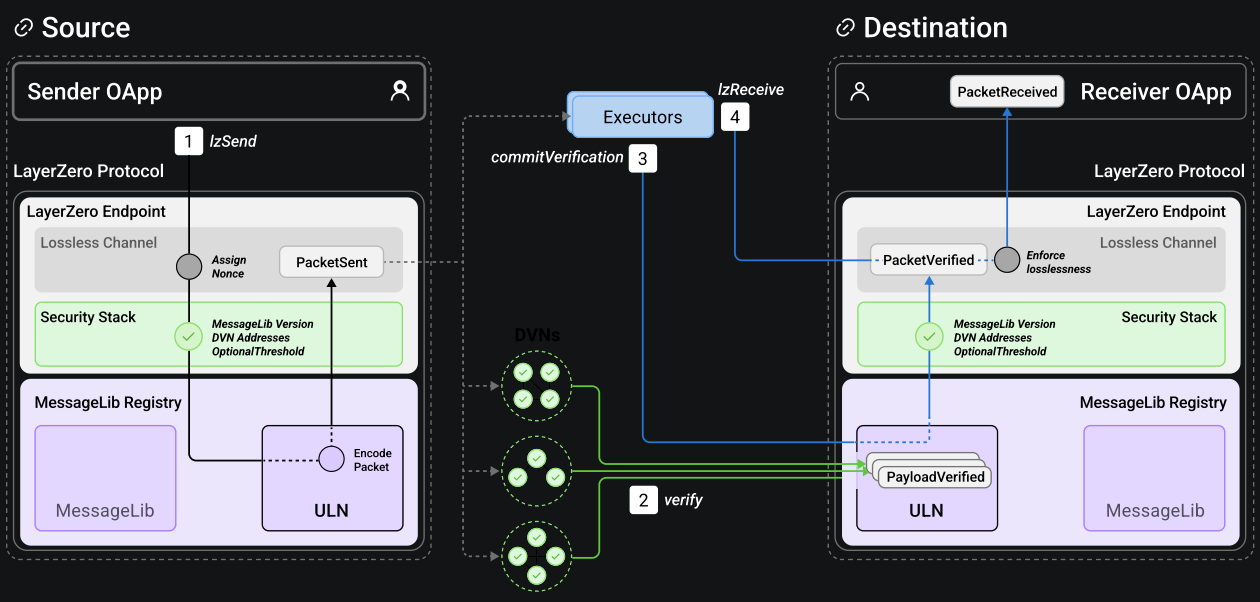
This step is essential because the protocol rules on either side of the transaction cannot fully guarantee message integrity across different blockchain environments.

Once verified, the message is delivered from one Endpoint to another, completing the transfer.

To further enhance security and composable functionality, LayerZero also incorporates the MessageLib Registry. This is an onchain repository of general-use contracts. These contracts, known as MessageLibs, are readily available for any project using LayerZero to call onchain.

Developers can select the appropriate MessageLibs from this repository to format and process messages, ensuring that the cross-chain messaging meets their specific security and functional requirements.

Figure 2: Architectural Overview Of LayerZero



Source: Layer Zero

Together, these components work to create a robust and adaptable framework for cross-chain transfers. Applications like Stargate utilize this architecture to support asset transfers across multiple blockchain networks.

LayerZero faces competition from several protocols in the cross-chain messaging and interoperability space. Key competitors include:

1/ Router Protocol: Router Protocol is a cross-chain messaging system that employs a mesh network architecture to enable communication between various blockchains. Router provides a range of tools, including its primary application, Voyager, a versatile widget, and an SDK known as CrossTalk.

2/ Axelar: Axelar is another protocol with its own cross-chain messaging tech called General Message Passing. GMP acts as a translator between different blockchain networks and lets developers call functions across chains. Axelar operates using a proof-of-stake consensus mechanism.

3/ Wormhole: Wormhole is a cross-chain messaging protocol designed to facilitate interactions between different blockchain networks. It operates through a network of 19 validators known as Guardians, who authenticate and verify messages sent across chains.

The protocol uses signed Verified Action Approvals (VAAs) as a core mechanism for confirming messages, again centralizing trust in the Guardians.

2.3 Threshold Cryptography bridges

The Threshold Network is a decentralized platform that employs threshold cryptography to create secure and private cross-chain bridges, most notably its tBTC v2 Bitcoin-to-Ethereum bridge. The network distributes key-holding responsibility among multiple participants through cryptographic shares.

A certain number of these shares—known as the threshold—must be deployed to sign transactions or decrypt data.

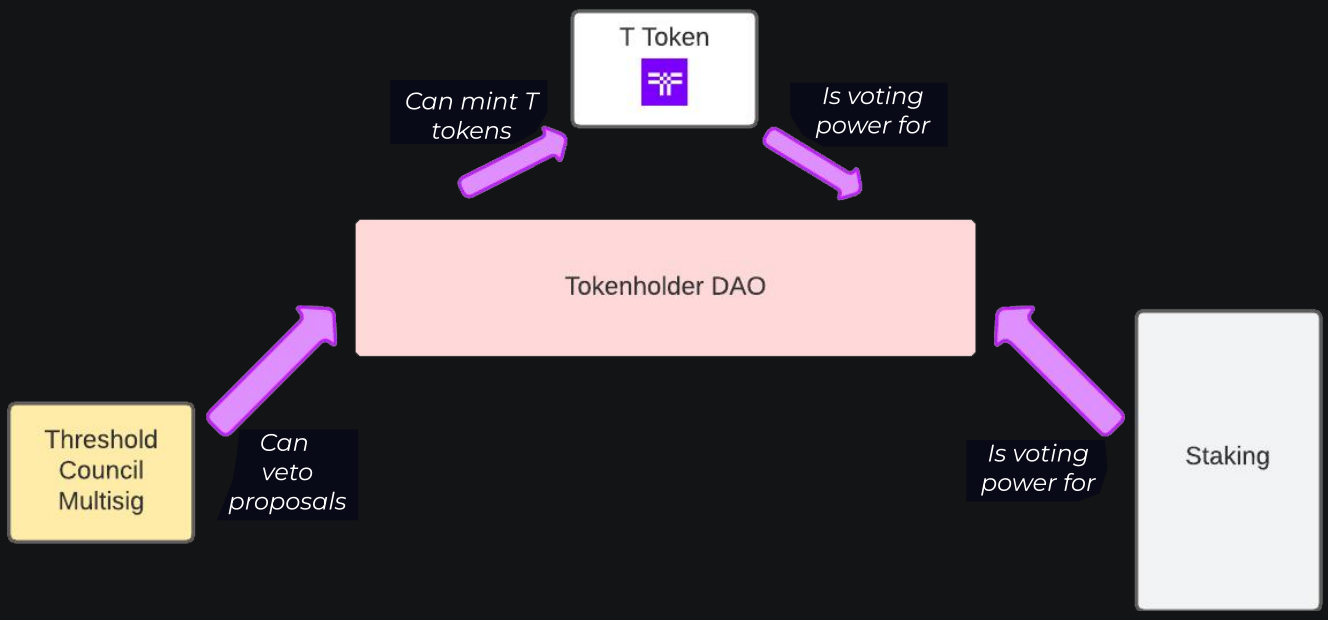
When pegging into tBTC, Bitcoin is deposited into the Threshold Bridge, where it is managed by a network of TSS node operators. These nodes are rotated weekly and contrast with regular federations like Liquid Peg out, which use a fixed group of entities and may be more static and prone to collusion.

To be eligible, participants must stake 40,000 T tokens—Threshold's governance token—and maintain at least 0.5 ETH for fees.

This staking requirement aligns their interests with network security, as penalties such as slashing can be imposed for infractions such as double signing or downtime.

However, it's important to note that slashing is not yet live on the mainnet. Therefore, TSS nodes remain permissioned for now, and Threshold's core contributors select operators based on stake size and reputation (Figure 3).

Figure 3: Threshold DAO



Source: Threshold Network

The fee structure for using tBTC is designed to be user-friendly. Currently, there is no fee for minting tBTC, which makes it accessible for users to convert Bitcoin into tBTC.

However, redeeming tBTC incurs a fee of 0.2%, which can be adjusted through the governance process as needed.

2.4 Portal to Bitcoin

Introducing BitScaler: Scaling Bitcoin for DeFi and Beyond.

// What is BitScaler?

Definition:

BitScaler is an innovative framework designed to enhance Bitcoin's scalability and programmability, enabling complex DeFi applications directly on the Bitcoin network. By leveraging advanced cryptographic techniques and innovative transaction structures, BitScaler addresses the inherent limitations of Bitcoin's base layer, opening the door for sophisticated financial instruments like Automated Market Makers (AMMs) and more.

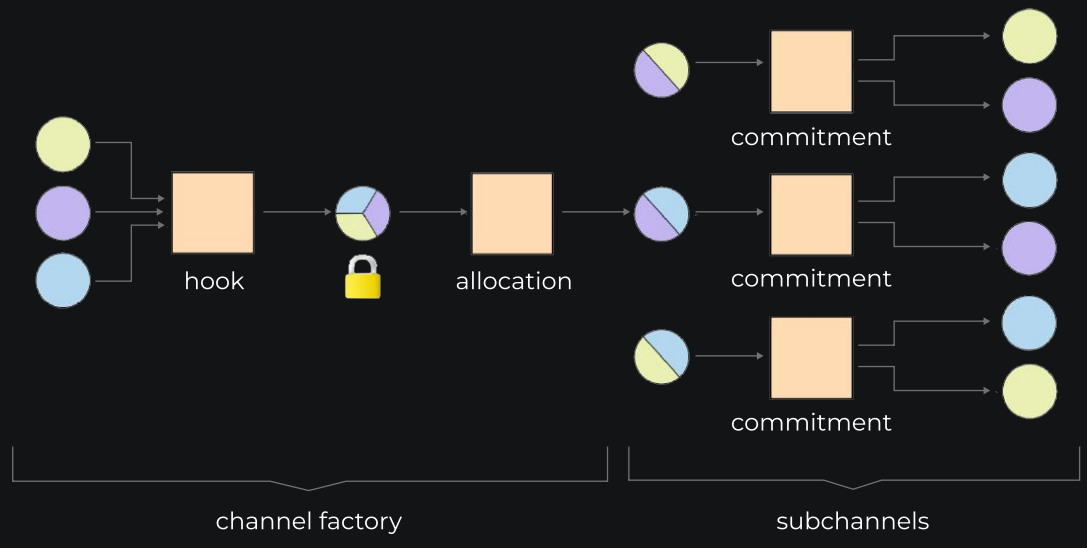
By using BitScaler on Bitcoin and corresponding smart contracts on other chains like Ethereum, complex cross-chain applications can be built while maintaining trust minimization and a non-custodial nature while maintaining the speed and user experience that centralized alternatives provide.

Key Components of BitScaler:

Customized Channel Factories

- **Definition and Purpose:**
  - Customized Channel Factories are multiparty payment channels that are formed offchain, with one onchain transaction, and limitless offchain P2P multiparty transactions, which surpasses the constraints of current Lightning Network limitations (minimum of 2 onchain transactions for every pair of peers) (Figure 4).
  - Enable multiple users to establish payment channels without each requiring an individual onchain transaction, significantly reducing the onchain footprint and associated fees. This is ideal for AMM-based DEX and DeFi use cases.
  - They act as a higher-layer solution (layer 3 or above) built on top of the Bitcoin network and duplex/multiplex channel L2.
  - Perfectly built for homogenizing liquidity in a pool vs. siloed liquidity locked up in channels, allowing the creation of AMMs. i.e., Multi LP liquidity can be used to satisfy a swap, which is not possible when 2 party channels like Lightning alone are used.
  - Delegated subchannels allow for laxed liveness requirements inherent in the Lightning Network without sacrificing security.
- **Channel Factory Structure:**
  - A group of users collectively locks funds into a single onchain transaction, forming a factory.
  - Within this factory, users can create numerous offchain channels between any pair of participants.
- **Transaction Efficiency:**
  - Aggregates multiple channels into a single transaction, eliminating the need for separate funding transactions.
  - Reduces the required onchain transactions from O(n) to O(1), where n is the number of channels.

Figure 4: Channel Factory With Subchannels



Source: BitScaler: Scaling Bitcoin for DeFi & Beyond

Benefits

- **Scalability:**
  - Significantly decreases the number of transactions that need to be recorded on the blockchain.
  - Reduces network congestion and transaction fees by up to 90%.
- **Flexibility:**
  - Users can open and close channels dynamically within the factory without additional onchain costs.
- **Liquidity Management:**
  - Homogenizes liquidity across channels, enabling effective liquidity monitoring and programmability.

Policy Scripts and Miniscript

- **Understanding Policy Scripts:**
  - Policy scripts are high-level representations of spending conditions for Bitcoin transactions.
  - They define the rules under which funds can be spent, such as multisignature requirements, time locks, or hash locks.
- **Miniscript Integration:**
  - Miniscript is a structured language for writing Bitcoin scripts in a way that is easier to analyze and compose.
  - It allows for the creation of complex scripts while ensuring they remain secure and efficient.
  - Serves as an intermediate layer between high-level policy descriptions and low-level Bitcoin scripts.
- **Implementation in BitScaler:**
  - BitScaler uses policy scripts and Miniscript to define the conditions for transactions within channel factories.
  - Enables the creation of customized, complex contracts that can be securely executed offchain.
- **Advantages:**
  - Security:
    - Ensures that all scripts adhere to Bitcoin's consensus rules.
    - Allows for formal verification of script correctness.
  - Composability:
    - Facilitates the combination of different script elements to create new functionalities.
  - Optimized Transactions:
    - Scripts can be simplified and optimized for lower fees and faster execution.

Solving the AMM Challenge on Bitcoin

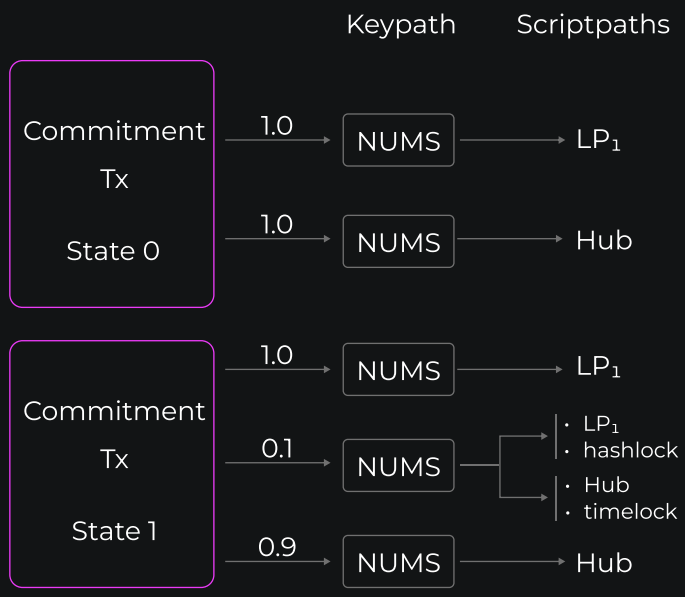
How BitScaler Solves the Automated Market Makers (AMMs) Implementation

- **Challenges on Bitcoin:**
  - Implementing AMMs on Bitcoin is difficult due to the lack of Turing-complete scripting and stateful smart contracts.
  - Traditional AMMs require the ability to manage liquidity pools and execute complex logic.
- **BitScaler's Solution:**
  - OffChain Execution:
    - AMM logic is executed offchain within the channel factories.
    - Reduces the need for complex onchain transactions.
  - Use of Payment Channels:
    - Trades are facilitated through customized payment channels between traders and liquidity providers (LPs).
  - Non-Custodial Delegation:
    - Users delegate certain functions to the network without giving up control of their funds. Validators cannot steal funds because the closing states are pre-committed and distributed to LPs.

- **Hook and Allocation Transactions:**
  - Hook Transactions:
    - Serve as the entry point for users into the AMM system.
    - Users commit funds and define their intended actions (e.g., swapping assets).
    - Lock the user's funds into the channel factory under specific conditions.
  - Allocation Transactions:
    - Distribute the committed funds according to the AMM's rules.
    - Determine how funds are allocated between different assets or liquidity pools.
    - Ensure that the user's desired trades are executed according to predefined parameters.
- **Trader and Liquidity Provider (LP) Channels:**
  - Trader Channels:
    - Channels between traders and the AMM system.
    - Allow traders to execute swaps and other operations without onchain transactions.
  - LP Channels:
    - Channels where liquidity providers commit their assets to the AMM.
    - LPs earn fees from trades executed by traders.
    - Can adjust their liquidity positions offchain, providing flexibility.
- **Benefits of This Implementation:**
  - Efficiency:
    - Minimizes onchain activity, reducing fees and improving transaction speeds.
  - Scalability:
    - Can handle a high volume of trades without congesting the Bitcoin network.
  - Security:
    - Funds remain under users' control, reducing the risk of loss due to hacks, mismanagement or validator collusion.
    - The worst-case scenario in a BitScaler-based DEX is a wait-out period in the case of validator collusion (in addition to collateral economic slashing security).
    - The worst-case scenario in every other cross-chain alternative (all bridges, messaging protocols, vaults, multisig custody) is the permanent loss of LP funds.

Atomic swaps using the AMM

The commitment transactions in each subchannel may gather HTLC outputs as one part of an HTLC-based atomic swap between the hub and the spoke for that channel. This is how traders are able to trade offchain against the AMM. The other half of the swap uses an HTLC equivalent smart contract on a Turing complete L1 or L2 or a Bitcoin sidechain. This is the key distinction between PortalToBitcoin and all other cross-chain approaches.



Hook and Allocation Transactions in Detail

- **Hook Transactions:**
  - Purpose:
    - Initiate the user's participation in the AMM.
    - Define the terms of engagement, such as the amount of funds committed and desired operations.

- Process:
  - The user creates a transaction that locks their funds into the channel factory.
  - The transaction includes the user's policy script, specifying conditions for fund usage.
  - Other participants in the factory (e.g., LPs, validators) acknowledge the transaction.

- **Allocation Transactions:**
  - Purpose:
    - Execute the distribution of funds according to the AMM's logic.
    - Reflect the state changes resulting from trades or liquidity adjustments.
  - Process:
    - Based on the hook transaction and subsequent offchain messages, the allocation transaction adjusts balances within the factory.
    - Updates are signed by all relevant parties to ensure consensus.
    - Only the final state needs to be recorded onchain when the factory is closed.

Trader and Liquidity Provider Channels

- **Trader Channels:**
  - Functionality:
    - Allow traders to interact with the AMM without incurring onchain transaction costs for each trade.
    - Enable rapid execution of trades and adjustments to trading strategies.
  - Operation:
    - Traders open channels within the factory by committing funds via a hook transaction.
    - Trades are executed offchain, with balances updated in real-time.
    - Traders can close their channels and settle balances onchain when desired.

- **Liquidity Provider (LP) Channels:**
  - Functionality:
    - LPs supply liquidity to the AMM, earning fees from the trading activity.
    - Can manage their liquidity positions dynamically, adjusting to market conditions.
  - Operation:
    - LPs commit assets to the factory through hook transactions.
    - The allocation transactions redistribute funds based on trading activity.
    - LPs can withdraw their liquidity or rebalance their portfolios as needed.

Non-Custodial Delegation

- **Concept:**
  - Non-custodial delegation allows users to delegate certain operations to other parties (e.g., validators or the network) without transferring ownership or control of their assets.
  - Users set predefined rules and conditions under which their funds can be used.

- **Implementation in BitScaler:**
  - Delegation of Channel Management:
    - Users can delegate the management of their channels to service providers or automated systems.
    - Service providers facilitate transactions on behalf of users while adhering to the users' policy scripts.
  - Maintaining Control:
    - Funds cannot be moved or spent outside the agreed-upon conditions.
    - Users retain the ability to revoke delegation at any time.

- **Advantages:**
  - Reduced Liveness Requirement:
    - Users do not need to be constantly online to manage their channels or respond to network events.

- Improved User Experience:
  - Simplifies participation in complex DeFi activities.
  - Makes advanced financial services accessible to a broader audience.
- Enhanced Security:
  - Delegation does not compromise asset security since private keys remain with the user.

Given the above, imagine how MP-HTLCs play in making smooth, CEX-like, L3 cross-chain swaps for spot markets and options markets possible between AMMs on different chains using the following toolbox.

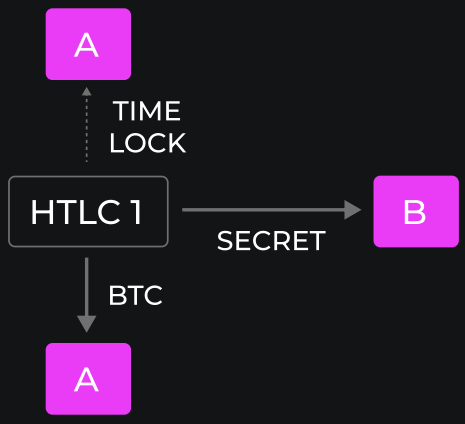
Learning Toolbox

Atomic swaps use Hash Time-Locked Contracts (HTLCs) to ensure that either both parties receive their intended assets or neither does, eliminating the risk of one party defaulting after receiving their funds.

Assume Alice wants to trade her Bitcoin for Bob's Ethereum. To initiate the swap, Alice generates a secret (also called a preimage) and creates its cryptographic hash pertaining to that preimage.

She then sets up an HTLC on the Bitcoin network that locks her funds. The contract stipulates that Bob can claim the Bitcoin if he provides the secret that matches the hash within a specified timeframe. If Bob doesn't claim the funds in time, Alice can reclaim her Bitcoin.

Figure 5: Schema Of The Commitment Transaction Sent From Alice To Bob



The HTLCs are set up to only allow withdrawals to specific blockchain addresses. Alice's contract on the Bitcoin network specifies Bob's Bitcoin address as the recipient, and Bob's contract on the Ethereum network specifies Alice's Ethereum address. This means that even if a third party somehow obtained the secret, they couldn't claim the funds because the contract wouldn't allow a transfer to their address.

Upon seeing Alice's contract, Bob creates a similar HTLC on the Ethereum network using the same hash.

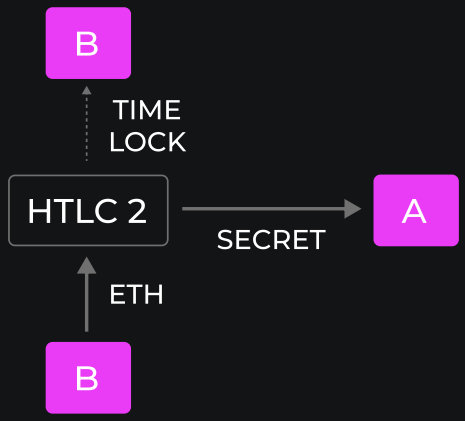
This contract allows Alice to claim the Ethereum if she reveals the secret or Bob to reclaim his Ethereum after the time lock expires.

To complete the swap, Alice reveals the secret to claim Bob's Ethereum. By doing so, she also exposes the secret to Bob, who can then use it to claim Alice's Bitcoin. To claim the funds, Bob must not only provide the secret but also sign the transaction with his private key corresponding to the specified address in the contract.

The time locks ensure that if any step in this process fails, both parties can recover their original funds after a set period.

This mechanism guarantees that the swap either completes fully or not at all, hence the term "atomic."

Figure 6: Schema Of The Commitment Transaction Sent From Bob To Alice



Portal's approach avoids the conventional lock-and-mint models used by some cross-chain solutions, where assets are locked on one chain and minted as a synthetic representation on another.

Instead, it uses the MP-Hash Time Lock Contracts (HTLCs) between the BitScaler-based AMM and other mirror smart contracts on other chains.

In the most basic form, HTLC, one party locks their funds with the hash of a secret. The counterparty creates a mirroring HTLC that is locked with the same hash. To claim funds, each party must reveal their respective secret within a set timeframe, ensuring the swap is completed fully or not at all.

Portal's goal is to create a seamless multichain AMM with the speed, composability, and low transaction fees of a CEX, as well as complete self-custodial security.

To ensure that neither LPs nor traders have to run all the full nodes of all supported chains on the client side, The Portal Network uses a distributed set of watchtowers who reach consensus on swap ordering, execution and broadcasting to the right L1 at the right time (Figure 7).

This is called the validator set. Selection of validator set, auction method, validator collateral etc, are referenced here. Validators in Portal run the Portal OS, which includes every supported chain's full node, a cross-chain messaging software called the coordinator and a PoS consensus mechanism on the Notary Chain.

The latter serves as an immutable record of the system's state and records all offchain swaps for audibility.

In addition to maintaining consensus on the Notary Chain, Validators route orders, maintain a synchronized decentralized order book, and oversee swap executions.

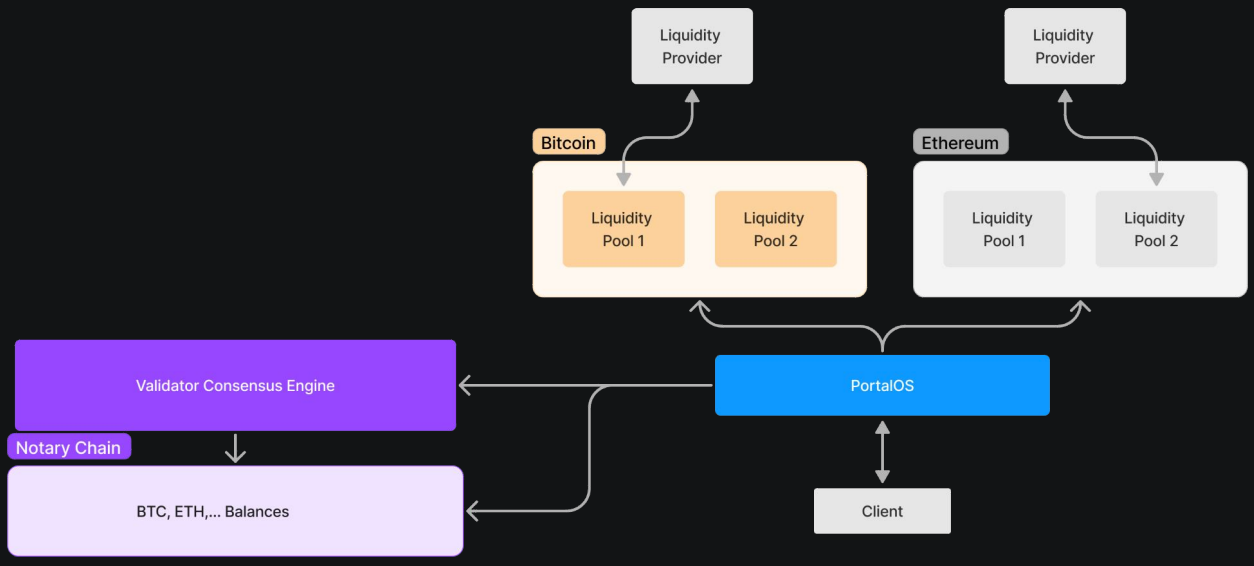
They verify swap requests by checking signature authenticity and fund availability on respective blockchains.

While some aspects, such as order routing and swaps, are facilitated through smart contracts, Validators actively ensure the system operates securely and efficiently by periodically posting cryptographic hashes of the current order book state to the Notary Chain.

The network supports up to 42 active Validators, with participation determined by their stake, further enhancing security through decentralized validation. Moreover, the compressed state of the notary chain is logged on the Bitcoin Chain as an OP_RETURN transaction chain to inherit Bitcoin's security against double spends or alteration of the Notary chain history.

This chain of transactions is signed at the change of every epoch by the outgoing validator set before the secure, offchain UTXO ownership transfer takes place prior to the new validator set coming online.

Figure 7: Portal's Core Network Operations



Source: Portal to Bitcoin docs

To enhance security of swaps, Portal uses Multi-Party Hash Time Lock Contracts (MP-HTLCs) on the Bitcoin network and equivalent contracts on other blockchains, such as Ethereum. Unlike traditional peer-to-peer HTLC swaps, Portal's system involves an element of trust in its infrastructure. However, the key differentiator still is the non-custodial nature of delegation of certain watchtower responsibilities from users to validators, which is a unique feature that is not available anywhere else.

MP-HTLCs use a Threshold Signature Scheme (TSS) to distribute the generation and management of cryptographic keys and secrets used in the atomic swaps among the federation members. The secrets distributed through TSS include the private keys used to sign transactions and the preimages used to create the hash locks of HTLCs.

In TSS, validators participate in TSS Keygen ceremonies and must cooperate to create and sign these elements, so no single validator holds complete control over the keys or secrets. This approach enhances security by eliminating single points of failure and requires multiple parties to collaborate for critical operations.

Portal DeFi operates on a Notary Chain architecture, which serves as the core database for all activities within the Portal Network. This chain manages and records cross-chain swap transactions, including trading pair registrations, validator auctions, slashing management, and liquidity pool balances.

When a user initiates a swap, the swap_intent() function triggers on the DEX contract account. Validators then call ADMM.register() on the Notary Chain and start a timer to handle the transaction.

Validators monitor external blockchains and PortalOS peers for events, automating this process through the PortalOS node and Coordinator. They do not need to track events manually, as the PortalOS node and Coordinator automate this process.

Validators must also witness and register events with a ⅔ majority to provide transaction metadata to all parties. If a validator approves an invalid transaction, other validators will detect and reject discrepancies.

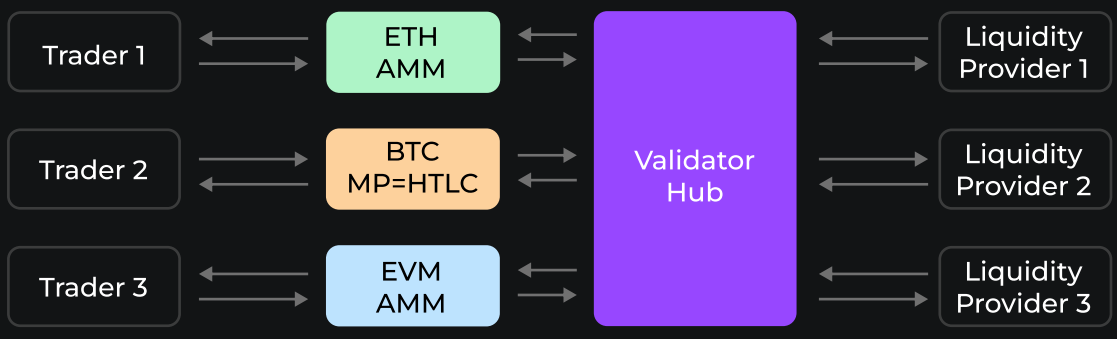
The system also implements penalties for dishonest validators, such as slashing their staked assets or removing them from the validator set. This creates a strong incentive for validators to act honestly and maintain the integrity of the network.

2.4.1 Portal's Automated Dynamic Market Maker (ADMM)

Building on this foundation, Portal facilitates swaps using an Automated Dynamic Market Maker (ADMM) deployed on each supported blockchain. The ADMM resembles Uniswap v3, supporting market, range, and limit orders but with enhanced efficiency. It dynamically adjusts to market conditions and utilizes external price feeds to determine asset values across chains (Figure 8).

Liquidity Providers (LPs) play a key role in this system by locking up native tokens to provide the necessary liquidity for asset exchanges. LPs create range orders by committing assets to liquidity pools. The ADMM then verifies LP capacity and updates the system's overall state. The range orders submitted by LPs divide a price span into ticks and distribute liquidity evenly across corresponding limit orders.

Figure 8: Simple Schema Of ADMM Operation

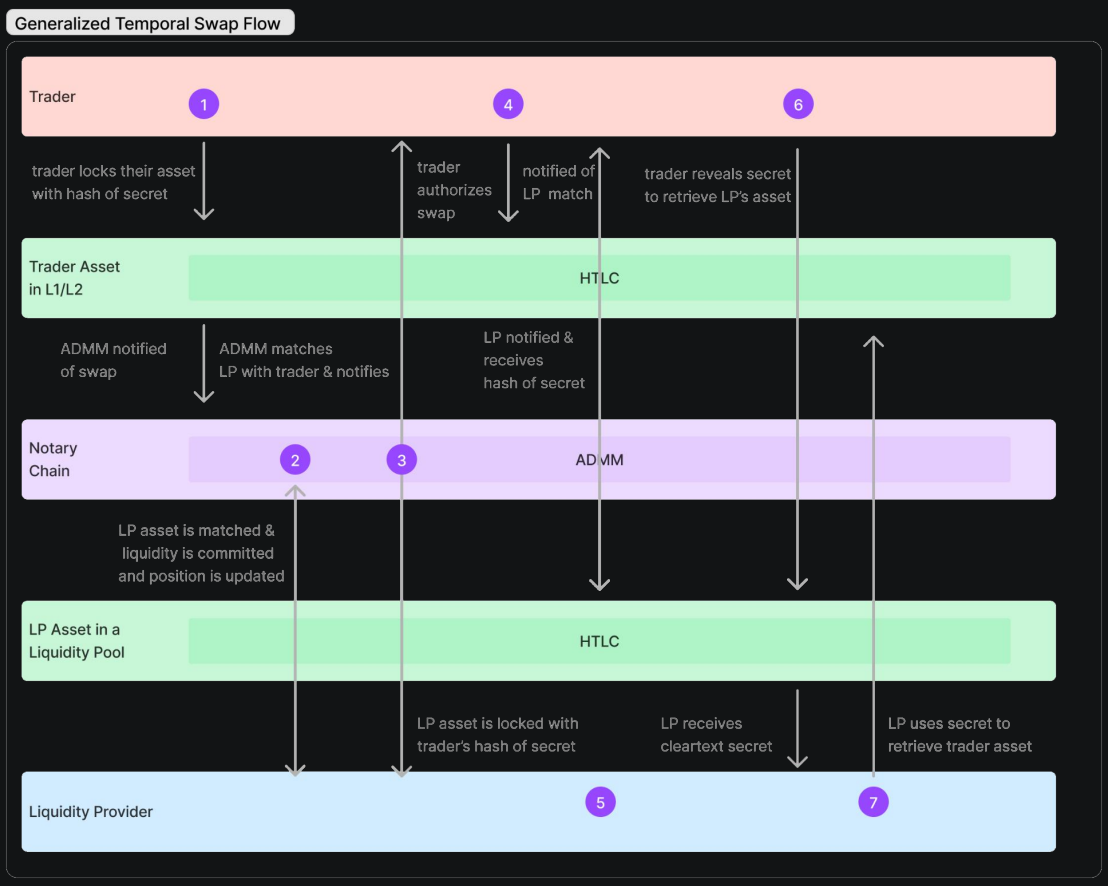


Source: Portal to Bitcoin docs

To initiate a swap, traders time-lock assets in a smart contract on the source chain. Validators register this intent on the Notary Chain, based on which the ADMM matches traders with LPs and provides a quote. LPs then create the second leg of a Hash Time Lock Contract (HTLC) by time-locking the requested asset. Traders complete the swap by revealing an atomic swap secret (Figure 9).

ADMM processes swaps in batches per block on the Notary Chain, reducing costs and front-running risks. It coordinates operations across blockchains using smart contracts on the Notary Chain and HTLCs on respective chains, which ensures atomic, non-custodial swaps.

Figure 9: Generalized Swap Flow Of Portal's ADMM



Source: Portal to Bitcoin's Docs

2.4.2 Portal DeFi's Tokenomics and Network Incentives

Portal DeFi intends to introduce an ERC-20 token called $PTB, which will serve as the platform's validator collateral and a utility token.

1/ It is the only collateral that the validators can use to participate in validator auctions, which happen every epoch, and it is used as their stake.

2/ In addition, $PTB is used as the fee token for swaps (and the fees paid are in native tokens that are converted to PTB at market price to be used in the notary chain for transactions, minimizing user friction through abstraction).

3/ The emission schedule for $PTB is based on a fixed supply model with a decaying issuance rate, similar to Bitcoin's halving mechanism. In the initial epoch, 1.45% of the existing supply will be minted, with the issuance rate decreasing by 1% per epoch until the total emission target of approximately 8.4Billion is reached. Half of the swap transaction fees are allocated to purchasing and burning $PTB tokens every epoch, creating a deflationary mechanism on top of the fixed supply.

Validators earn rewards through newly minted $PTB tokens triggered by network events such as epoch completions or upgrades. This incentivizes active participation in network governance and operations. Validators are also subject to a slashing mechanism, which penalizes negligent behavior, such as extended offline periods or failure to fulfill network duties, by reducing their staked tokens.

These slashed tokens are permanently removed from circulation. Moreover, liquidity providers are paid a percentage of emissions in each block, along with light nodes and supernodes. This helps keep the network incentivized to decentralize.

At launch, Portal DeFi will support the Bitcoin, Lightning, Ordinals, BRC20, Ethereum, Arbitrum, Aeternity blockchains and other Ethereum layer 2 blockchains, as well as many BTC layer 2 solutions. Portal DeFi aims to incentivize Liquidity provision by aggressively bootstrapping the network and reducing spreads. This is implemented through Liquidity Providers (LPs), who, by increasing the depth of liquidity, earn 50% of the swap fee and the second-highest percentage of block emissions after validators. This, in turn, can create competitiveness and attract traders.

For a Full analysis of the Portal To Bitcoin Tokenomics proposal and a thorough technical report by Dr.John Conley, see here.

3. Conclusion

Bitcoin's position as the preeminent store of value in the crypto space remains undeniable. Yet its integration within DeFi has faced notable limitations. While Ethereum currently dominates the DeFi space and holds over $48 billion in total value locked (TVL), Bitcoin's DeFi TVL remains at a modest $1.9 billion. This highlights the significant headroom for Bitcoin-native DeFi to expand.

In this report, we examined four networks — Chainlink CCIP, LayerZero, Threshold Network, and Portal-To-Bitcoin. Each offers a distinct approach to cross-chain interoperability, but all projects share a common goal of facilitating seamless interactions between disparate blockchain environments. They have chosen different trade-offs between security, decentralization, and efficiency.

Chainlink's CCIP, for example, relies on decentralized oracle networks to transmit data across chains. However, even decentralized oracles introduce vulnerabilities that could compromise transaction integrity if exploited.

LayerZero employs a modular framework for message verification and transmission. While this provides a lot of flexibility for creating cross-chain infrastructure, the reliance on Oracle-Relayer pairs raises concerns about potential collusion. The Threshold Network mitigates some of these risks by distributing control over cryptographic keys across multiple participants through threshold cryptography.

This model reduces the likelihood of centralized failures but currently relies entirely on permissioned nodes.

Portal to Bitcoin provides a novel solution with its BitScaler innovations, multiparty HTLCs and a non-custodial validator model, which is specifically designed to resolve Bitcoin's interoperability challenges. Unlike other protocols that depend on lock-and-mint mechanisms or synthetic assets, Portal enables direct, non-custodial atomic swaps without the need for wrapped tokens or custodial bridges.

This structure eliminates many of the risks associated with traditional bridging mechanisms, such as liquidity fragmentation and the counterparty risks of custodial models. While Portal introduces a degree of trust in its infrastructure, this is no different from any base layer technology or blockchain, and it significantly advances security by ensuring that validators cannot steal user funds, even in worst-case scenarios.

As seen in the report, each network offers unique strengths and caters to different aspects of cross-chain interoperability. The choice between them depends on the specific requirements of the use case—whether prioritizing security, flexibility, decentralization, or trustlessness. Portal's focus on Bitcoin interoperability, combined with its innovative solution to bridging challenges, positions it as a critical long-term player in the future of cross-chain DeFi.

Disclaimer

This document is for information only and does not constitute investment advice, an investment recommendation, or a solicitation to buy or sell — it is merely a summary of key aspects of the Cointelegraph Report. In particular, this document is not intended to replace individual investment or other advice.

The information contained in this publication is based on the knowledge available at the time of preparation and is subject to change without notice. The authors were diligent with their selection of information but assume no liability for the accuracy, completeness or timeliness of the information provided.

Past performance is not a guide to future performance. Values may fall or rise, and you may not get back the amount you invested. Income from investments may fluctuate.

Cointelegraph does not endorse and is not responsible for or liable for any content, accuracy, quality, advertising, products or other materials on this page. Readers should do their own research before taking any actions related to the company.

Cointelegraph is not responsible, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with the use of or reliance on any content, goods, or services mentioned in this publication.

ADDITIONAL CONTACTS

Questions, Comments or Customer Service



research@cointelegraph.com