Bool Network Technical Reliability Audit Report

27/03/2024

✉ contact@scalebit.xyz   https://twitter.com/scalebit_

ScaleBit

Content

Overview

Bool Network is a network that utilizes Zero-Knowledge Proof-based Verifiable Random Function (ZKP-VRF), Trusted Execution Environment (TEE), and an independent data availability layer to keep its network's overall reliability, security, and privacy. Specifically, Bool Network can be regarded as middleware, existing as a validator network between the L2 network and the BTC network, helping BTC L2 projects establish reliable asset transfer channels. The Bool Network has the potentially to be the infrastructure in L2 ecosystem, which includes:

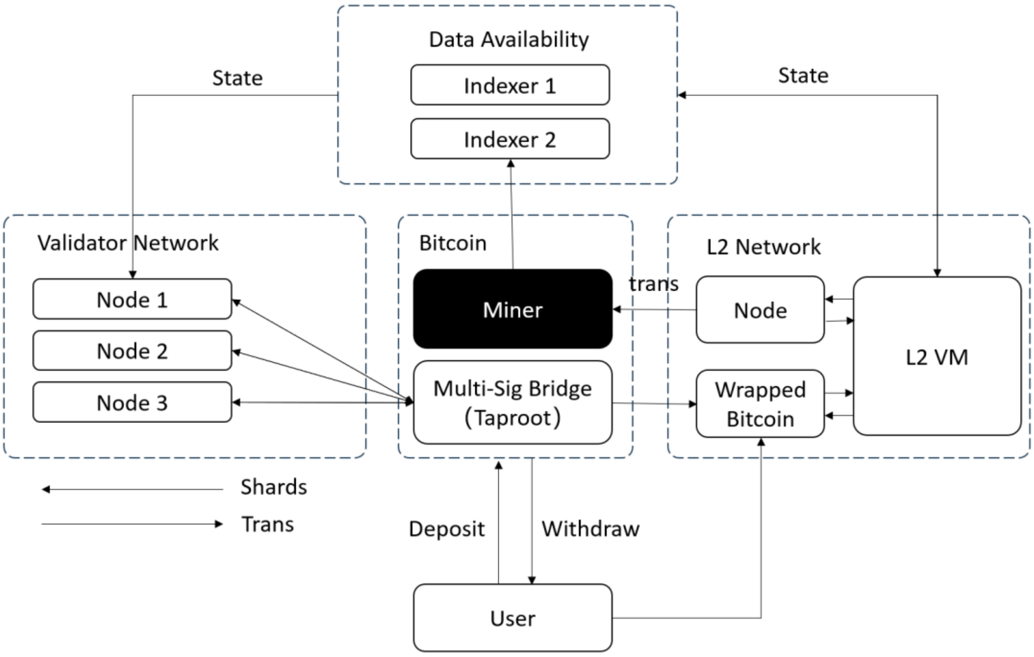
- A trusted oracle, providing data and verification services for more BTC L2 projects.
- A trusted cross-chain bridge, safely transferring assets to other token networks (e.g., from BTC to ETH).

The goal of this report is to analyze the overall framework and components of Bool Network, to define the function of each different module, and to conduct a theoretical analysis to ensure they can complete their tasks correctly, efficiently, and reliably. Subsequently, we will evaluate the overall performance of Bool Network, considering potential inherent risks. Finally, we will compare Bool Network with other implementations, showcasing its advantages and potential weaknesses, and conclusion.

Architecture

Typical BTC L2 Architecture

Before delving into the architecture of Bool Network, which primarily acts as middleware between BTC L1 and L2, it's essential to understand the typical architecture of BTC L2 solutions. BTC L2 solutions are designed to enhance the scalability and efficiency of transactions on the Bitcoin blockchain while ensuring security and decentralization. The relationship between the different modules is illustrated in the figure below:



A Typical BTC-L2 solution (Sovereign Rollup) consists of the following components:

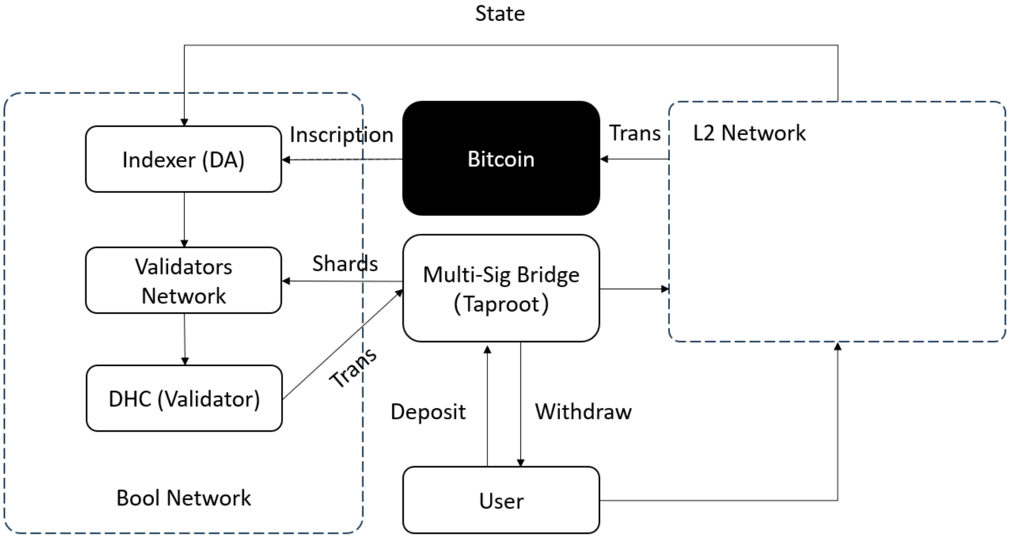
1. **Layer 1 (Bitcoin Blockchain):** The base layer where all Bitcoin transactions are recorded. It's secure and decentralized but has limitations in terms of scalability and transaction speed.

2. **Assets Bridges:** These are protocols that allow the transfer of assets between the Bitcoin blockchain (L1) and L2 solutions. They lock assets on L1 and mint corresponding assets on L2, enabling users to transact with higher speed and lower fees.
3. **Validator Network:** This network consists of nodes that validate transactions on the L2 solution. Validators are responsible for maintaining the integrity and security of the L2 network, often using various consensus mechanisms to agree on the state of the network.
4. **L2 Networks:** These are separate blockchain protocols built on top of the Bitcoin blockchain. They process transactions more efficiently than L1 by using various techniques, such as state channels, sidechains, or rollups. After processing, the final state or a batch of transactions is settled back on the L1 blockchain.
5. **Data Availability Layer:** An essential component ensuring that all transaction data on L2 is available to nodes on the network. This layer prevents data-withholding attacks and ensures the network can verify the correctness of the L2 state.

The Bool Network Architecture

Bool Network adheres to this paradigm, with its core focus on enhancing the reliability of the validator network to move closer to a trustless schema. Specifically, in Bool Network, it is assumed that the implementation of the assets bridge is through a multi-signature account, meaning the assets bridge account is locked by a threshold signature made up of multiple private key fragments. The security of the multi-sign assets bridge directly depends on the reliability of the holders of the private key fragments. The goal of the Bool Network is to make it technically difficult for nodes within the validator network to collude and behave maliciously.

Bool Network integrates the Data Availability (DA) layer with the validator network, enabling L2 networks to directly complete asset staking and verification through it. This integration facilitates a more streamlined and secure approach to managing and verifying L2 transactions. The Overall construct of the Bool Network is demonstrated in the following figure:



1. **Direct Asset Staking and Verification:** By integrating DA with the validator network, Bool Network allows for the immediate staking of assets on the L2 network. This means users can lock assets in the assets bridge with confidence, knowing that the assets' state and transactions will be accurately reflected and verified on L2.
2. **Enhanced Security and Trust:** The combined use of ZKP-VRF and TEE technologies within the validator network ensures a high level of security and trust. These technologies provide a secure, random selection of validators and enforce the integrity of transaction processing, making collusion and malicious activities extremely difficult.
3. **Improved Data Availability:** With the DA layer integrated into the validator network, Bool Network ensures that all transaction data on L2 is readily available for verification. This availability is crucial for maintaining the transparency and security of the network, allowing any discrepancies to be quickly identified and resolved.

4. **Efficiency and Scalability:** The integration allows L2 networks to operate more efficiently by streamlining the process of asset staking and verification. It reduces the complexity and potential bottlenecks associated with asset transactions, leading to improved scalability and faster transaction speeds within the BTC ecosystem.

In summary, the integration of the DA layer with the validator network in Bool Network not only simplifies the asset staking and verification processes but also significantly enhances the overall security, efficiency, and functionality of L2 networks within the Bitcoin ecosystem.

Extra Component

Apart from the validator and DA network, Bool Network also includes its L2 SuperChain through Bool Stack. Bool Stack's components not only define specific layers within the Bool Network ecosystem but are also embedded as modules into existing layers. Bool Stack focuses on running L2 blockchain infrastructure, in theory, it encompasses various layers above the base blockchain, including block explorers, messaging mechanisms, governance systems, and other tools. This comprehensive development stack provides robust support for building and expanding the Bitcoin and L2 blockchain ecosystems, fostering technological innovation and interoperability within the ecosystem.

- Bool Stack uses the Ethereum Virtual Machine (EVM) to host contracts, allowing accounts to interact with these contracts.
- Bool Stack adopts the Nominated Proof-of-Stake (NPOS) method for consensus and governance, based on which it issues and utilizes native tokens.
- Bool Stack will use a native data availability layer and leverage the Bitcoin network for data storage.

Essential Module

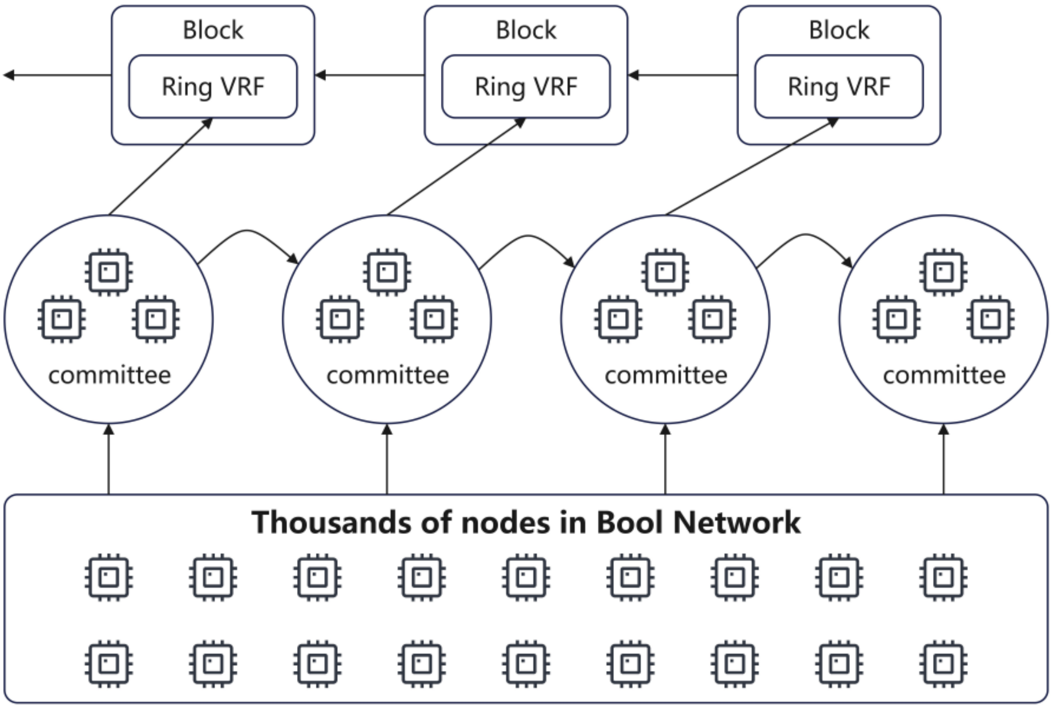
The main components of Bool Network include two parts: the dynamic hidden committee (DHC) and the data availability layer (DA). Among these, the validator network is the core of Bool Network's security, while the other two parts are relatively secondary due to the existence of many mature solutions.

Dynamic Hidden Committee（DHC）

The Bool Network integrates the validator network, and it's also known as the DHC, because the nodes that actually perform the validation function represent a subset of the entire Bool Network's validators. This setup is designed to prevent collusion and malicious actions within the network. The operation of this protocol is as follows:

1. The entire model operates in rounds, with each round ultimately producing a block that records how the assets guarded by Bool Network will change.
2. Validators within Bool Network are required to be equipped with Trusted Execution Environments (TEEs) to execute the protocol.
3. At the start of a round, validators first verify the correctness of each transaction through the data availability network.
4. Once all transactions are confirmed, validators in the Bool Network must run a multi-party secure computation within the TEE, which combines Zero-Knowledge Proofs (ZKPs) with Ring VRF to generate a series of random numbers and reach consensus among the nodes.
5. Based on the random numbers generated in the previous step, Bool Network selects a portion of the nodes to form the committee for that round, known as the Dynamic Hidden Committee (DHC).

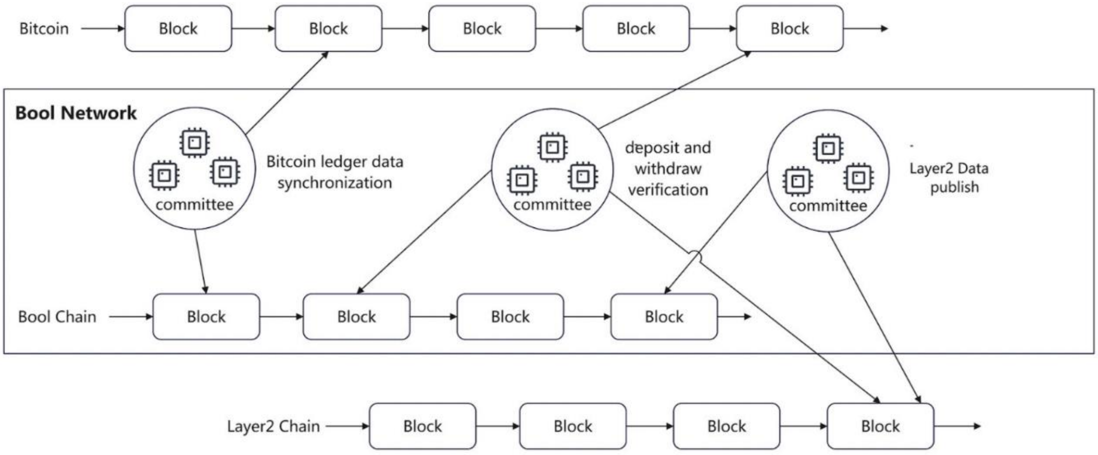
6. Once the committee is established, its members collectively generate the block for that round and operate on the assets in the L1 bridge.



This mechanism enhances the security and integrity of the Bool Network by ensuring that only a dynamically selected, unpredictable subset of validators participates in the consensus and validation processes for each round. This approach reduces the likelihood of collusion and attacks, making the network more robust against potential security threats.

The Data Availability (DA) Layer

The DA in the Bool Network is used to ensure that transaction data for Bitcoin and L2 networks are accessible and verifiable by all nodes within the network. If data are not available, other nodes cannot verify transactions, potentially leading to inconsistencies and security issues in the network. The relationship between DHC and DA is shown in the following figure:



Bool Network adopts an advanced data availability layer, responsible for managing and providing transaction data across all chains within the Bitcoin and L2 networks, and feeds to the DHC with specific functions including:

- The DA layer is in charge of managing and providing transaction data for all chains, supporting interconnectivity and secure sharing between different chains.
- The Bool Network utilizes Merkle trees and hash functions to create immutable digests of data, allowing nodes to verify data consistency.
- Data availability is fundamental to ensuring the consistency and security of the Bitcoin ecosystem, especially crucial within modular stacks that provide multi-layer shared security infrastructure.

Security Analysis

Overview

From previous analyses, it's evident that, from an L1 implementation perspective, Bool Network's bridge employs a multisig scheme. Thus, even though its validator network could theoretically consist of nearly a thousand nodes, the actual controllers of the assets are the members of the Dynamic Hidden Committee (DHC) within the validator network. Therefore, the core of Bool Network's security hinges on the advanced anonymity of the DHC, meaning that the validator network cannot know the members of the DHC, nor can the DHC's member nodes know their own involvement in the protocol state. If this condition is met, it can prevent nodes from colluding to steal assets, thereby better protecting the assets on the L1 bridge.

In the following subsection, we listed the essential properties that the Bool Network should satisfy, and evaluated if it meets the requirements. In addition, we offered suggestions in response to our concerns. We will evaluate Bool Network's security from three different perspectives: its ability to resist **malicious attacks, collusion misbehavior,** and **node failures**. Among these, the anonymity of Bool Network will be a key factor for the first two security concerns.

Malicious Attack

All networks are susceptible to malicious attacks, specifically encompassing two scenarios: attacks on consensus, such as double-spending attacks; and attacks on the network, such as denial-of-service attacks. In terms of consensus attacks, the key to prevention lies in the strength of the data's association with the Bitcoin network. As for network attacks, the crux is whether the nodes are sufficiently dispersed and decentralized. We will consider the issue of malicious attacks from these two perspectives.

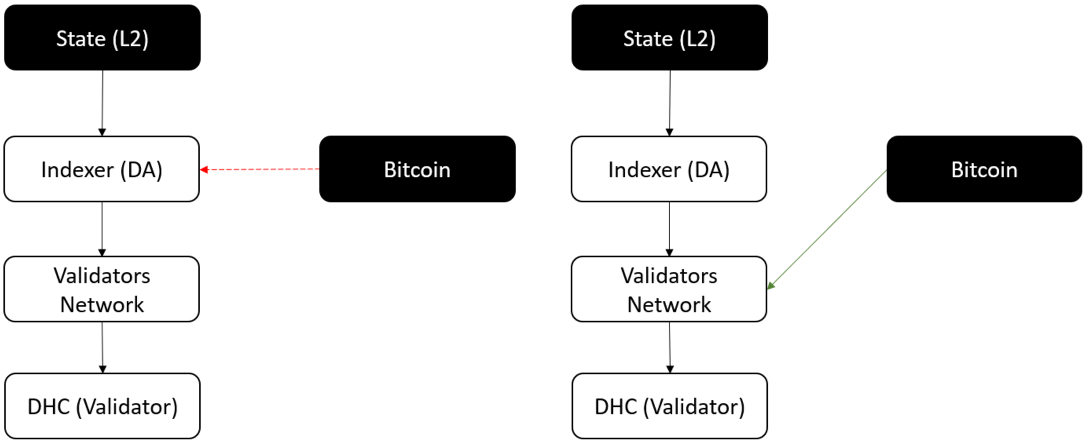
Bitcoin Related

This property is required **The Block in the Bool Network is finalized by the Bitcoin Network**. It indicates the DHC should only accept data that is confirmed in the Bitcoin Network. In this case, the DHC in the network actually receives data from two different sources:

- The Bitcoin Network
- The DA Layer

Apparently, when DHC uses a confirmed block from the Bitcoin Network, the incoming state change can be granted. However, when Bool Network possibly takes unconfirmed data directly from the DA layer, the state change may face the risk of being invalid. The suggested (Green) and unsuggested

(Red) workflow is shown in the following figure:



Generally, we suggested that the DHC should take the Bitcoin blocks directly, or use only confirmed data from the DA layer. When the first approach, requires the DHC running parts of the DA layer itself. We believe it can ensure safety, however, it heavily loads the Validator. The second approach is indeed more effective, however, requires a trusted DA layer that will not occupied by malicious parties. Both solutions are feasible. Which one to use will depend on the conditions of the Bool Network itself.

DDoS Resistance

This property is required **The Bool Network is decentralized and robust simultaneously**. Decentralized indicates the Bool Network should be permissionless, while the full-node, light-node, client should be free to establish. The robustness indicates the total number of nodes in the network is large enough. Meanwhile, the committee should not be predictable, which will break the robustness of the network.

Regarding the first point, the Bool Network can indeed operate in a decentralized manner and does not have any theoretical prerequisites for participation. Although not all nodes can join the Decentralized Hash Committee (DHC), any node can join the Bool Network using the P2P network protocol and become a potential validator. However, we have also observed that since the Bool Network utilizes a TEE environment to run the DHC protocol, nodes might need to employ specialized hardware to properly join the Bool Network. In this regard, although the Bool Network cannot run on arbitrary hardware, it has adopted middleware for TEE development, enabling it to support various trusted computing devices, such as ARM's Trusted Zone and Intel's SGX, as much as possible.

Concerning the second point, since the Bool Network allows nodes to freely join and leave, it can be expanded to a sufficient number of nodes. Additionally, since the DHC controlling the cross-chain bridge does not include a large number of nodes, excessive communication overhead is not generated. In theory, the Bool Network can support hundreds to thousands of nodes. After the election of the DHC, the use of ZKP effectively protects the results of the Ring-VRF, making it impossible for committee members to predict or know the outcomes. External attackers would have to launch DDoS attacks against all nodes to paralyze the committee, as targeted attacks on DHC members are unfeasible. Therefore, we believe that the Bool Network has a good resistance to network-layer attacks.

Collusion Misbehavior

The key to preventing collusion and malicious behavior among nodes lies in the randomness of the election process and the knowability of identities. When the election process can be manipulated in some way, malicious nodes will be able to easily control the network; similarly, when misbehaving nodes can obtain each other's identities, they will be able to assess the feasibility of collusion.

Randomness

This property requires **In a situation where the majority of nodes are honest, they can generate reliable, non-manipulable, and verifiable random numbers**. We noticed that Ring VRF, as a technology that has been rigorously proven and widely validated in practice, is considered fully capable of achieving this effect.

In a nutshell, Ring-VRF combines the anonymity features of ring signatures with the randomness and verifiability of VRFs. It allows a member of a group to produce a random number and proof of its validity without revealing which member generated it. In blockchain protocols, Ring-VRF can be used to select validators or leaders in a way that is both random and verifiable, but without revealing the identity of the selected party. This enhances privacy and security. In addition, in this case, the Ring-VRF is even more secure with ZKP, where the identity of DHC is also under protection, and will not be revealed. In this case, committee elections based on VRF are inherently difficult to manipulate and sufficiently random. It is believed that there are no theoretical security issues in this part.

After the formation of the Dynamic Hidden Committee (DHC), the members of the committee cannot know each other's identities, nor can they know their own identities, and the committees will be different in each round. Under the perfect TEE assumption, since the entire protocol runs within the TEE and nodes cannot access the state inside the TEE, they cannot know their own identities or the identities of any other members. Thus, the key lies in whether the TEE environment used by Bool Network can ensure that its internal state cannot be known. If the internal state of the TEE can be accessed by some means, the following scenarios could occur:

- Any node could know whether it is a member of the committee for that round.
- Nodes attempting to collude could communicate off-chain to know whether they are members of the committee for that round.

However, since the execution process of the TEE cannot be tampered with, knowing each other's identities would not allow for the transfer of user assets, but only allow for a DDoS attack on that round. It is recommended to strictly inspect the TEE to ensure that its environment meets the ideal security assumptions. simultaneously, it is necessary to ensure a sufficiently large number of nodes in the network to prevent similar committees from being used in different rounds.

Assets/Access Control

This property is required **Any node would be unable to maliciously manipulate the assets in the assets bridge by any means**. Since users cannot change the running process in the TEE environment, they cannot collude in the validator network to maliciously manipulate user assets. However, two aspects that need to be cautious.

The first aspect indicates the DA layer should not be fully trusted. As suggested, if the data availability network is controlled by malicious nodes, it is still possible to maliciously manipulate user assets. If validator nodes in the TEE environment fully trust data from the data availability layer, the layer could maliciously manipulate assets in the assets bridge by fabricating data to construct false and erroneous transactions. However, It is recommended to perform secondary verification of data from the BTC network within the TEE to mitigate this risk.

Regarding the second point, the TEE (Trusted Execution Environment) cannot be regarded as entirely secure. Several known attack methods can compromise the security assumptions of a TEE. A typical attack is the Side-Channel Attack. Even though TEEs provide an isolated execution environment, they still share some physical resources with the non-secure world, such as cache and power supply. Attackers could exploit these shared resources to perform side-channel attacks, inferring sensitive information by analyzing patterns in resource usage or electromagnetic emissions.

Additionally, since some TEE software seeks authorization from manufacturers, there is also the potential for malicious control by upstream providers. In response, the Bool Network minimize the requirement for security authorizations and attestation inside the bool network, therefore strengthen the security design and performance of the TEE environment.

Node Failure

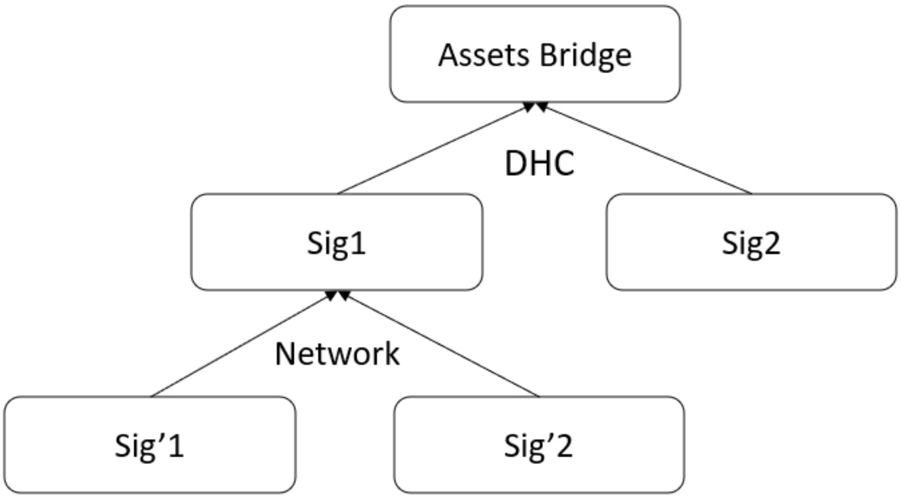
Node failure is a possibility in any network. Clearly, the Bool Network needs to ensure that the protocol can still operate smoothly in the event of partial network failure; and in the case of a complete network failure, users can retrieve their assets. These two points can be classified as **fault tolerance** and **escape hatch**, respectively.

Fault Tolerance

Any network is susceptible to malicious attacks, which specifically can include two scenarios: attacks against consensus, such as double-spending attacks, and attacks against the network, such as denial-of-service (DoS) attacks. For consensus attacks, the key to prevention is ensuring that its data has a sufficiently strong link to the Bitcoin network. As for network attacks, the key lies in whether the nodes are sufficiently distributed and decentralized. We will consider malicious attacks from these two perspectives.

This property requires that the network can still operate normally even if a certain number of nodes fail. Regarding node failure, it can be divided into two different scenarios: failure of nodes in Bool Network, and failure of nodes in the DHC. For the first scenario, due to Bool Network having a robust network and the DHC being dynamic, ordinary node failures have a minimal impact on Bool Network. For the second scenario, since the DHC actually controls the assets bridge, users will not be able to withdraw assets in that round if the entire DHC fails. Also, since the DHC internally uses Multi-Party Computation (MPC) to control the private key, the possibility of restoring the private key by other nodes will be lost if all DHC nodes fail, leading to all assets being locked. Although the probability of all DHC nodes failing is small, it still exists.

Under the premise of an ideal TEE environment, we suggest adopting a multi-level aggregated signature scheme. That is, the signatures within the DHC could also be aggregated and restored by the majority of nodes. The advantage of this approach is that no node still has the ability to independently restore the private key, and the efficiency of the DHC would not be affected. With the protection of the TEE environment, the security of these keys can be maximized.



Overall, we believe that Bool Network has good fault tolerance, but the failure of DHC nodes could lead to severe network issues. In an ideal scenario, there should be a way to distribute keys so that in the event of DHC failure, the network could skip that round and select a new DHC in the next round.

Escape Hatch

Despite Bool Network's fault tolerance, in the aforementioned extreme situations, it may still face scenarios where assets become locked. Therefore, users need a method to forcefully exit their assets at the Bitcoin L1 level. Bool Network proposes utilizing Bitcoin's Taproot feature and time-lock mechanisms. By integrating The HTLC within the script, Bool Network enables functionalities for time-bound asset unlocking or signature-based asset unlocking.

For instance, implementing a one-year time-bound unlock would require asset unlocking solely through a DHC's signatures within this period. In the extremely unlikely scenario of substantial loss of private key shares managed by the DHC during this period, asset retrieval remains possible upon the time lock expiration, enabling retrieval from a collectively managed account.

Although this solution may require a considerable amount of time to exit a user's assets, considering that this approach is also adopted by most L2 project asset bridges;

and at the same time, the probability of Bool Network failure is minor. Therefore, we believe that the design of this escape hatch mechanism is effective and reasonable.

Comparison

In this chapter, we compare the Bool Network with other BTC L2 solutions. While Bool Network Focuses on the construction of a **trustless bridge**, we will pay special attention to this certain aspect.

Existing Solution

The assets bridge is the heart of any L2 solution. It's vital to ensure the assets of users can be safely deposited and withdrawn, while the bridge must be secure enough against **malicious attack, collusion, and node failure** The notable existing solutions of the assets bridge are:

1. **MPC**

The most classic solution involves multiple trusted parties safeguarding the key fragments of the assets bridge. When it's necessary to operate on the assets, different participants utilize a Multi-Party Computation (MPC) protocol for signing.

2. **Taproot Multi-Sig**

Typically, this approach employs a Taproot account as the assets bridge. Moreover, the key is split into numerous fragments, which are then aggregated through a consensus mechanism by a validator network with many nodes for signature aggregation.

3. **DLCs**

Different from the previous two approaches, each user possesses a unique Discreet Log Contracts (DLCs) based assets bridge. Users can construct numerous Conditional Execution Transactions (CETs) off-chain, defining the potential outcomes within the cross-chain bridge beforehand, which are then executed by an oracle network.

4. **Bridgeless Solution**

This method allows for off-chain asset exchange without an assets bridge, securing the transaction through cryptographic approach, such as state channels (lighting network).

Metric

To effectively compare these solutions, establishing metrics for evaluation is necessary. Based on industry consensus around key standards, with a primary focus on security, we have developed the following dimensions for evaluation:

1. **Access Control**
   - How the Assets Bridge is controlled, whether this control is sufficiently secure and decentralized.
2. **Data Source**
   - The origin of data from trusted third parties, notaries, the Bitcoin network, or other Data Availability (DA) layers.
3. **Escape Hatch**
   - How assets can exit the Assets Bridge in the event of an L2 network failure.
4. **State Verification**
   - The verification mechanisms used for data produced in L2, and the network to which the verifiers belong.
5. **Functionality Extensibility**
   - Whether it supports running smart contracts, virtual machines, and other Turing-complete scripts in L2.
6. **Network Efficiency**

- Whether the network can support high throughput and confirm transactions quickly.

These metrics provide a comprehensive framework to assess and compare the effectiveness and robustness of different L2 solutions or features within the Bitcoin ecosystem. They highlight the importance of security, decentralization, reliability, and scalability in developing and evaluating blockchain technologies, particularly those enhancing Bitcoin's functionality through Layer 2 solutions.

Summary

We have adopted a comparative analysis of the above approaches against Bool Network's solution, represented in a table format for clarity:

Feature	MPC	Taproot	DLCs	Bridgeless	Bool Network
Access Control	Moderately-Decentralized	Highly-Decentralized	User-Controlled	User-Controlled	Highly-Decentralized
Data Source	Trusted Parties	Bitcoin Network	Oracle Network	Bitcoin Network	Bitcoin Network + DA Layer
Escape Hatch	MPC Protocol	Time-lock	Time-lock	Cryptographic	Taproot + Time-lock
State Verification	Off-Chain Verification	Off-Chain Verification	Oracle Verification	Cryptographic	Cryptographic + MPC + TEE
Functionality Extensibility	High	High	Moderate	Limited	High
Network Efficiency	High	High	Moderate	Moderate	High

This comparison showcases how each solution addresses key aspects such as access control, data source, escape mechanisms, state verification, functionality extensibility, and network efficiency. Bool Network aligns closely with the high standards of network efficiency and functionality extensibility while ensuring decentralized access control, secure and versatile data sourcing through Bitcoin Network and a DA layer, and robust state verification mechanisms employing TEE technologies. The inclusion of Taproot and time-lock mechanisms for the escape route also provides a secure method for asset retrieval in extreme scenarios. However, considered the aim of Bool Network is to secure the validation network, therefore, its ecosystem has not yet shown promising grown.

Conclusion

Bool Network aims to become an indispensable infrastructure within the BTC L2 landscape, with its core innovation focused on the validator network segments. Through two key technologies, Zero-Knowledge Proof-Verifiable Random Function (ZKP-VRF) and Trusted Execution Environment (TEE), it ensures the security of assets in the bridge under the premise that only a few nodes are trustworthy. This is achieved by concealing the identities of nodes and enforcing protocol computations. On this basis, Bool Network also includes its native data availability and L2 network solutions. Through a series of comparisons, Bool Network provides reliable protection for assets, and its overall technological approach has a promising outlook. Simultaneously, we have also raised some considerations regarding security. Among them, the TEE environment is a crucial part of Bool Network's security assumptions, requiring strict inspection to ensure it performs as expected. Meanwhile, the data availability layer should also be trusted to minimum the risk.

Disclaimer

This report is based on the scope of materials and documents provided, involved with the concepts, architecture and key schemes, without the review of codes, libraries and implementations. Meanwhile, this report formed with a limited review at the time provided. Results may not be complete and do not include all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.