DeepSafe: A Bitcoin Verification Layer

DeepSafe Team

December 2023

Abstract

Bitcoin's growth paved the way for innovations like Ordinals protocol and BRC-20, hinting at asset issuance potentials within its framework. However, Bitcoin faced hurdles in expanding its use cases and scalability. Enter DeepSafe, a decentralized Bitcoin verification network, leverages advanced cryptography to boost Bitcoin's scalability, security, and cross-chain abilities. This paper presents a programmable framework for Bitcoin Layer 2 on DeepSafe, fostering secure asset issuance and cross-chain experiences across heterogeneous blockchains. DeepSafe's decentralized approach ensures Bitcoin's scalability without altering its consensus rules, fostering swift and secure Bitcoin Layer 2 development and interoperability while embracing community-driven governance.

1 Introduction

Bitcoin, proposed by Satoshi Nakamoto's seminal white paper in 2008 [1], revolutionized the economy by enabling trustless cross-border financial transactions devoid of intermediaries. Its foundational tenets encompass censorship resistance, immutability, and decentralization. However, the fundamental protocol underpinning Bitcoin has encountered limitations, notably in its capacity to support sophisticated functionalities, particularly concerning on-chain programmability and composability.

In response to these limitations, alternative blockchains emerged, most notably Ethereum, conceptualized by Vitalik Buterin in 2013 and formally launched in 2015 [2]. Ethereum's pioneering introduction of smart contract capabilities heralded a significant technological leap, paving the way for a diverse spectrum of decentralized applications (DApps). Post-2020, with the rise of Decentralized Finance (DeFi) and Non-Fungible Token (NFT), Ethereum has solidified its position as a leader in smart contract blockchains, while witnessing the emergence of other smart contract public chains such as Solana [3], Avalanche [4], among others. Nonetheless, Bitcoin remained primarily confined to serving as digital gold, emphasizing value storage.

Despite undergoing substantial upgrades, such as the activation of the Segregated Witness (SegWit) in 2017 [5], which tackled specific scalability issues by segregating witness data from the basic block, and the Taproot upgrade in 2021 [6] [7] [8], aimed at enhancing performance, privacy, and smart contract functionalities, Bitcoin struggled to explore diverse and flourishing use cases within its ecosystem.

The advent of Ordinals protocol in 2023 [9] marked a pivotal turning point in Bitcoin's capabilities. This protocol facilitated the binding of diverse data types, encompassing text, images, videos, etc., to a singular "Satoshi" [1], thereby embedding inscriptions into Bitcoin transactions. Subsequently, the development of BRC-20 protocol based on Ordinals [10] generated ripples in the cryptocurrency sphere. While causing congestion on the Bitcoin chain, it highlighted the potential for asset issuance, scalability, smart contract creation, and more intricate functionalities within the Bitcoin framework, underscoring the exigency for scalability enhancements in the Bitcoin ecosystem.

Amidst these developments, DeepSafe emerged as a pioneering solution that integrates advanced techniques such as Multi-Party Computation (MPC), Zero-Knowledge Proof (ZKP), and Trusted Execution

[1] A Satoshi is the smallest unit of Bitcoin, named after Bitcoin's pseudonymous creator, Satoshi Nakamoto. One Bitcoin is divisible into 100,000,000 Satoshis.

Environment (TEE). It aims to address Bitcoin's scalability and programmability challenges while augmenting its decentralization. As an extension of the Bitcoin verification layer, it introduces a range of innovative technologies and protocols, offering new possibilities for blockchain security, scalability, and decentralization.

At the core of DeepSafe is the concept of supporting the construction of more secure and efficient Bitcoin Layer2s (L2) through key components like Crypto Random Verification Agent (CRVA), Data Availability Layer (DA), and Execution Layer. Its architecture aims to ensure the security of the Bitcoin verification layer while providing an innovative way to handle cross-chain transactions and asset exchanges.

2 Background

Before delineating the innovative design architecture of DeepSafe, this chapter will enumerate the challenges and developmental requisites confronting the current Bitcoin network. Additionally, it will explore prevalent scalability resolutions and their corresponding successful implementations.

2.1 Challenges

2.1.1 Scalability

Over an extended period, Bitcoin has grappled with the challenge of scalability. Despite being one of the most valued and secure cryptocurrencies, it has gradually distanced itself from its initial aspiration of becoming a "peer-to-peer electronic cash system". Persistent constraints such as limited network capacity ($1MB$), confirmation duration (averaging 10 minutes per block), and transactional velocity (requiring more than 6 blocks for finality) continue to encumber Bitcoin's capacity for processing substantial transaction volumes.

Even with the introduction of SegWit in 2017, a measure that moderately augmented network capacity to a maximum of $4MB$, it fell short in entirely alleviating congestion during periods of heightened transactional loads. Particularly notable was the fervor surrounding BRC-20, which led to pronounced congestion in Bitcoin transactions, with peak gas fees surpassing 300 sat/vB and instances of multiple block times exceeding 1 hour [2]. Consequently, the imperative of bolstering the network's throughput and scalability stands as a paramount concern in the present milieu.

However, unlike programmable blockchains such as Ethereum, the Bitcoin network represents a "stateless" ledger, incapable of executing intricate smart contracts or fostering composability. To foster diverse decentralized applications on Bitcoin, a programmable framework integrating"state, computation, and verification" is imperative to augment its functionality and adaptability. Presently, Bitcoin grapples with several inherent characteristics:

- **State**: Bitcoin's current Unspent Transaction Output (UTXO) set solely computes real-time"balances", while foundational state components crucial for constructing contracts remain unattainable.
- **Computation**: Bitcoin's core computational abilities are confined within UTXO script unlocking conditions. Yet, these constrained capabilities struggle to articulate complex business logic.
- **Verification**: While Bitcoin full nodes verify UTXO balances and script signatures, their scope is limited to fundamental verification, incapable of assessing the specific execution effects of these logics.

These constraints impede the diversified application development within the Bitcoin network, necessitating a more profound programmable infrastructure to propel its progression.

[2]Mempool, https://mempool.space/graphs/mining/block-fee-rates

2.1.2 Security

The network security and stability of the Bitcoin network directly impact the incentive mechanism and revenue sources for miners. Bitcoin's economic model employs a halving mechanism directly affecting miners' earnings. Presently, the primary source of miners' income stems from block rewards. However, with the fourth halving in 2024, the reward per block will reduce from 6.25 BTC to 3.125 BTC. This underscores the limitations of a model reliant solely on block rewards within the current landscape. The introduction of Ordinals protocol has increased the proportion of transaction fees in miners' income, accounting for approximately $10\% - 30\%$, emerging as their second-largest revenue source [3]. This escalated proportion to some extent reflects the contribution of transaction fees to miners' earnings, bearing significant implications in incentivizing miners to uphold the security of the network.

Nevertheless, the surge in the number of transactions on the network has also brought forth challenges such as dust attacks and spam inscriptions, highlighting certain challenges within the existing model. To address these challenges, the migration of assets to the L2 networks of Bitcoin for liquidity and settlement has emerged as an avenue for improvement. Such migration not only alleviates pressure on the underlying network but also offers users a faster, more cost-effective transaction experience, thereby expanding Bitcoin's utility scenarios. This sustainable consumption scenario based on Bitcoin's L2 network holds the potential to enhance the stability and consensus of the Bitcoin network, ensuring its long-term secure operation.

2.1.3 Programmability

In the realm of the blockchain industry, smart contract developers predominantly concentrate within the Ethereum Virtual Machine (EVM) ecosystem. According to publicly available data, as of 2023 [4], approximately 50% of global blockchain developers engage in development activities on the EVM. Relative to developing on the native Bitcoin chain, these developers encounter elevated technical barriers and complexities in expanding the ecosystem.

Therefore, leveraging a decentralized L2 network of Bitcoin while providing an EVM-compatible environment is considered a more desirable solution. The primary aim of Bitcoin scalability solutions is to allure a greater number of developers and users, thereby expanding the Bitcoin ecosystem. To achieve this objective, reducing entry barriers is deemed a paramount principle. Intricate designs or high thresholds could significantly augment the difficulty of attaining success in Bitcoin scalability solutions.

2.2 Related Work

The Bitcoin scalability solutions are primarily categorized into three types: State channels, Sidechain, and Client-side validation.

2.2.1 State channels

Based on creating direct channels between two or more transaction participants, state channels allow them to conduct multiple transactions rapidly within the channel without requiring confirmation for each transaction on Bitcoin.

Lightning Network [11] is designed as a solution to address the scalability issues and high transaction fees within the Bitcoin network. By creating bidirectional payment channels, it enables users to conduct fast and low-cost transactions outside the Bitcoin main chain, without the need to record each transaction on the Bitcoin main chain. While the Lightning Network does not support smart contract functionality, it ensures reliability through the introduction of SegWit and instantaneous payments. Introduced in 2016 as a test network, its purpose was to resolve Bitcoin's transactional scalability issues

[3] Mempool, https://mempool.space/graphs/mining/block-fees
[4] Developer report, https://www.developerreport.com/

and facilitate instant payments. Its core concept revolves around establishing bidirectional payment channels, allowing for rapid Bitcoin transfers between two Bitcoin accounts with minimal fees. During transactions, the Lightning Network generates four transaction proofs, containing records of transfers between both parties and the nullification of the previous transactions between the parties. This process involves two interactions with the Bitcoin network: opening and closing payment channels. Transactions require mutual agreement and signatures from both parties to ensure transaction confirmation reliability. Once the payment channel is established, after each payment completion, both parties obtain private keys to nullify the old contracts. Additionally, the Lightning Network interweaves payment channels into a payment network through Hashed Time-Lock Contracts (HTLCs). This method allows transferring BTC from $Account_a$ to $Account_b$ and subsequently paying BTC to $Account_c$, ultimately completing the transfer from $Account_a$. However, due to the capacity limitations of transfer channels, the Lightning Network is currently primarily utilized for small-scale payments and transfers, focusing on addressing Bitcoin's payment issues.

2.2.2 Sidechain

Bitcoin sidechains are independent blockchains connected to the Bitcoin main chain, enabling users to transfer assets between them. Through a mechanism of locking on the main chain and minting on the sidechain, users can engage in faster and more cost-effective transactions on the sidechain.

Stacks [12] is a platform positioned as a smart contract layer for Bitcoin, aiming to establish smart contracts and decentralized applications (DApps) within the Bitcoin ecosystem. Launched in 2018, it introduced a mechanism called"Stacking" designed for cross-chain interactions with Bitcoin. This mechanism essentially operates as a centralized mapping method, associating sBTC tokens issued on the Stacks network with Bitcoin. While Stacks does not explicitly position itself as a sidechain, in essence, it constructs a new chain operating outside the Bitcoin network, possessing an independent governance structure and transaction model. Despite Stacks offering an innovative sidechain model to enhance Bitcoin's functionality for decentralized application development and operation, its adoption of the Clarity language and the centralized nature reliant on the Stacking mechanism result in a total value locked (TVL) in the ecosystem currently below $25 million.

Rootstock [13], founded in 2018, initially started as a Bitcoin sidechain but later integrated with RIF Labs and shifted focus towards DeFi. Emphasizing the smart contract realm, it boasts high compatibility with Ethereum. RSK's operation involves bidirectional anchoring for interaction with Bitcoin, featuring EVM compatibility, fast transactions, and merged mining. Despite its 10-second transaction speed and 90% support from the Bitcoin network's hash power, issues of centralization persist due to hash locks, restricting the amount of BTC available for cross-chain transactions using RSK. RSK still employs a POW consensus algorithm, limiting its ecosystem development despite its 2018 launch, resulting in relatively delayed ecosystem growth.

Liquid [14], introduced by Blockstream in September 2018, utilizes L-BTC and supports the creation and transfer of other assets [15]. Similar to RSK, it adopts the M-of-N federated multi-signature asset custody, emphasizing a rapid transaction network while supporting confidential transactions. Liquid achieves Bitcoin scalability through a sidechain solution, providing rapid, high-value, and anonymous transfers for exchanges and trading platforms. The issued L-BTC conducts asset transfers with BTC through bidirectional anchoring, requiring multiple confirmations and custodians for processing. Similar to the Lightning Network, Liquid employs mechanisms to ensure the network's long-term operation. Launched by Blockstream as a Bitcoin L2 network, Liquid operates as a Bitcoin sidechain, primarily servicing institutions and asset issuers. Its Bitcoin cross-chain solution exhibits relative centralization, relying on 11 authenticated multi-signature nodes to custody BTC, resembling a permission-federated blockchain. Prioritizing security and privacy, Liquid requires permission for access, functioning as a consortium chain solution. While rational for institutional services, a decentralized and permissionless

Bitcoin Layer 2 might hold greater development prospects to gain extensive support and adoption from the Bitcoin community and crypto users.

2.2.3 Client-side validation

The client-side validation scheme continues the mainnet UTXO model, allowing off-chain clients to handle more complex transactions. However, its lack of bidirectional verification and constraints with the Bitcoin mainnet have resulted in its underdeveloped state.

RGB [15] is a Bitcoin Layer2 protocol built upon Bitcoin's UTXO and Lightning Network infrastructure. Its core design comprises UTXO state compression encapsulation, client-side validation, and the execution of non-shared smart contracts on the Lightning Network. However, RGB has yet to accomplish the encapsulation of operational data into each Bitcoin UTXO, resulting in increased difficulty in asset verification. Despite breakthroughs in scalability, privacy, and programmability, RGB faces challenges in verification complexity, blockchain security, and interoperability. Its latest iteration, RGB v0.10, has made significant upgrades in consensus layers, standard libraries, and user experience by introducing the Strict Types new type system, enhancing the convenience of smart contract development. However, the RGB ecosystem remains in its nascent stages, marked by high developer learning costs, slow project iteration pace, and verification efficiency concerns. The market acceptance and feasibility of RGB in the future will require further examination and time to validate.

2.2.4 Other approaches

BitVM [16], proposed in 2023 as a BTC L2 solution, remains in the theoretical phase. Its fundamental premise involves executing fraud proofs akin to optimistic rollups on Bitcoin scripts, enabling challenges in cases of contentious asset transactions. The smart contract layer of BitVM operates off-chain, with individual smart contracts not sharing state. Recently, the lead of the ZeroSync project published a whitepaper titled"BitVM: Computing Anything on Bitcoin", outlining a solution that aims to grant Turing completeness to Bitcoin without altering the network's consensus rules. This has garnered attention due to Bitcoin's relative weaknesses in smart contracts and complex computations, areas that BitVM attempts to address. Prior solutions often required modifications to consensus rules, whereas BitVM preserves outcomes off-chain through fraud proofs and an optimistic mechanism. It involves roles such as Provers and Verifiers, employing logical gates and challenge mechanisms for fraud detection. While BitVM presents novel prospects for smart contracts, challenges regarding efficiency, scalability, and feasibility persist, such as concerns over function expression efficiency and channel construction methodologies.

3 Protocol Overview

In the preceding chapters, the discourse centered on the unavoidable challenges confronted by scalability proposals within the Bitcoin ecosystem, encapsulated by the paradigm of the impossible trilemma. This trilemma delineates the delicate equilibrium required between security (inheritance of security protocols from Bitcoin's foundational layer), scalability (facilitating smart contracts enabling intricate and composite business logic), and developer accessibility (utilization of languages prevalent among mainstream blockchain developers). In light of these deliberations, the introduction of DeepSafe surfaces—a programmable framework distinguished by a"state + computation + verification" mechanism. Its primary objective lies in providing a convenient infrastructure across all blockchains for the seamless construction of Bitcoin Layer 2 solutions within the domain of DeepSafe.

3.1 Overview

DeepSafe is a permissionless, decentralized, and secure Bitcoin verification layer that aims, within the premise of not altering Bitcoin's consensus rules, to securely and decentralize the expansion of the Bitcoin network, thereby fostering prosperity within the Bitcoin ecosystem.

The transaction throughput of Bitcoin has long been a crucial concern for users. Despite Bitcoin's clear advantages in security and decentralization, its limited transaction speed restricts its ability to effectively handle a large volume of transactions. This issue is an integral part of the blockchain impossible trilemma. To address this challenge, one of the primary solutions is the adoption of Layer 2 technologies. However, due to Bitcoin's inherent lack of smart contract functionality, current Layer 2 solutions commonly encounter issues related to centralization.

To overcome these challenges, we propose DeepSafe, a decentralized and secure Bitcoin verification layer driven by MPC-based distributed key management. It aims to address the constraints on Bitcoin's transaction speed. DeepSafe comprises an evolving agent of hidden members. To safeguard the identities of agent members, we introduce the Ring Verifiable Random Function (Ring VRF) protocol [17]. In this protocol, the genuine public keys of VRF instances are concealed within a ring. Furthermore, to ensure the privacy and integrity of key components, all key management procedures are executed within a Trusted Execution Environment (TEE), such as Intel SGX. This proposal seeks to mitigate Bitcoin's transaction speed limitations while upholding its decentralization and security.

3.2 Technical Perspectives

3.2.1 Network architecture

DeepSafe constitutes a Layer 2 scaling solution aiming to address scalability and transaction speed issues within Bitcoin. It operates as a permissionless protocol, enabling participants to establish cross-chain payment channels facilitating swift and cost-effective transactions.

The architecture of DeepSafe manifests as a layered structure encompassing multiple components and levels that collaborate to realize efficient transactions. The primary architectural elements of DeepSafe are illustrated in Figure 1:

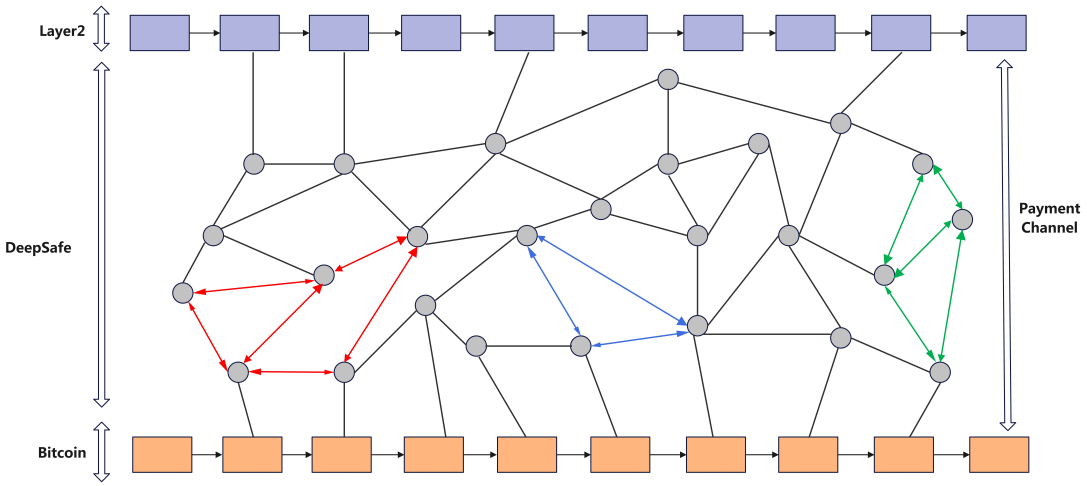

Figure 1: Network architecture of DeepSafe.

- **Bitcoin layer**: The Bitcoin network forms the foundational layer of DeepSafe. Participants can create payment channels on Bitcoin and subsequently commit final settlements to Bitcoin when necessary.

- **Payment channel**: Channels established on Bitcoin link two participants (Bitcoin and Layer 2) through private channels. These channels can be bidirectional, facilitating multiple transactions within the channel. Opening and closing channels involve transactions on Bitcoin.
- **Crypto Random Verification Agent layer**: CRVA represents a core component within DeepSafe, ensuring the security of payment channels. Comprised of multiple verification nodes within DeepSafe, as illustrated by the nodes connected with red, blue, and green edges in Figure 1, CRVA conceals node identities and undergoes periodic node rotation. Moreover, two agents can create a bidirectional payment channel.
- **Verification Node layer**: DeepSafe constitutes a network of verification nodes following a permissionless pattern. Each verification node runs the core program of DeepSafe alongside a Bitcoin full-node program. Verification nodes offer verification services to one or multiple Crypto Random Verification Agents and additionally provide Bitcoin ledger data services.
- **Extension layer**: This layer interacts with DeepSafe. It communicates with the underlying channels and verification nodes, executes transaction payment requests, and interacts with Bitcoin when necessary.

3.2.2 Functional architecture

DeepSafe, as a verification layer for Bitcoin, adheres to the modular blockchain design philosophy. Its entire architecture encompasses multiple potential layers of a modular blockchain stack, as detailed in Figure 2. These layers, when utilizing DeepSafe's CRVA (Crypto Random Verification Agent) and DA (Data Availability) layers, respectively undertake Bitcoin's self-custody and the availability storage of Bitcoin transaction-related data. Moreover, the architecture includes various independent Rollups, such as Sovereign OP Rollup and ZK Rollup, which directly leverage DeepSafe's settlement layer.

Simultaneously, it also supports operational Rollups, for instance, enabling Ethereum's Layer 2, Arbitrum, to function as both Ethereum's Layer 2 and Bitcoin's Layer 2. In this context, it relies on DeepSafe to provide verification of relevant transaction data on Bitcoin while leveraging its existing liquidity for settlements.

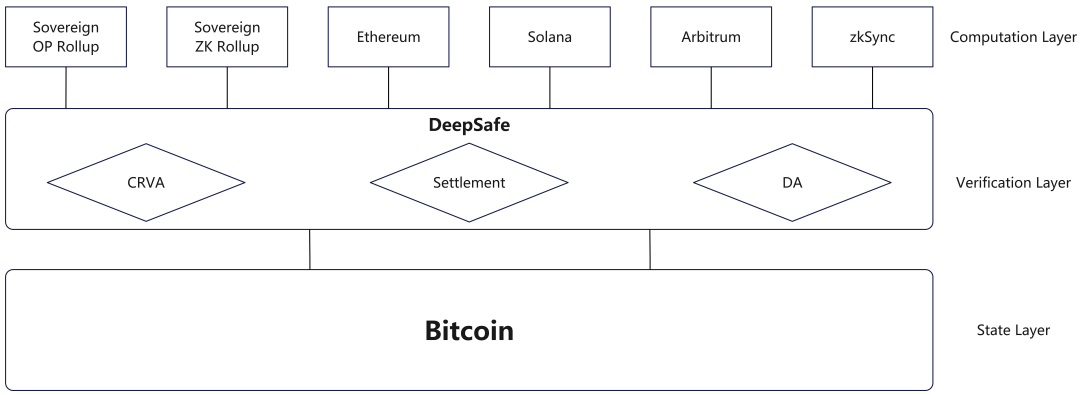

Figure 2: Functional architecture of DeepSafe.

In the modular stack, sovereignty refers to each component (such as applications and layers) having an independent governance structure that does not overlap with others. This can be seen as a form of separation, where each stack part operates under its governance mechanism. The advantages of sovereignty in a modular stack include:

1. **Independence**: Each component can have its own governance rules and decision-making processes, allowing it to make decisions independently of other components.

2. **Flexibility**: Different components can experiment with various governance models that suit their specific needs. This flexibility might lead to governance structures that are more suitable and efficient.

3. **Efficiency**: If a specific application or layer faces issues or requires upgrades, its governance can address these concerns without affecting other components. This targeted approach can result in faster issue resolution.

4. **Anti-interference**: The sovereignty principle helps prevent interference between different parts of the stack. Changes or decisions in one governance entity do not automatically affect other parts.

5. **Innovation**: Independence in governance allows for experimentation and innovation within different parts of the stack. This can foster creativity and evolution in governance practices.

The most crucial aspect is that while sovereignty brings these advantages, coordination, and interoperability mechanisms remain paramount to ensure the overall functionality of the modular stack. When necessary, independent components should seamlessly interact, and there might be instances where cross-component governance decisions are vital for the entire network's interests. Striking a balance between sovereignty and coordination is crucial for the success of a modular stack.

3.3 Core Modules

3.3.1 Crypto Random Verification Agent

Crypto Random Verification Agent (CRVA) stands as one of the central and pivotal concepts within DeepSafe, enabling it to achieve a security level equivalent to or surpassing that of Bitcoin. Each agent is responsible for managing the private keys of specific blockchains, including Bitcoin, for the verification of messaging security.

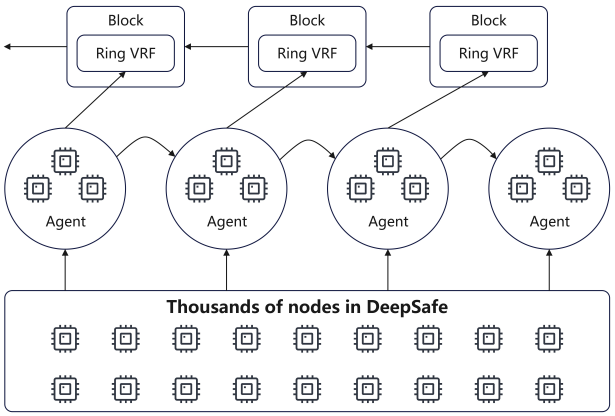

Figure 3: Crypto Random Verification Agent (CRVA).

Introducing the unique Ring VRF election algorithm ensures the privacy and randomness of agent members' identities. Notably, all agent procedures run within a Trusted Execution Environment (TEE) to ensure the confidentiality and integrity of relevant components [5]. The core technical aspects, as depicted in Figure3, encompass:

[5]Verification network in DeepSafe operates permissionlessly, allowing any node to freely join or exit. Although requiring configuration of TEE-related hardware and staking a certain amount of tokens, without the need for excessive collateral, it presents a relatively low entry threshold.

- The network comprises X TEE nodes, from which N nodes are randomly selected using Ring VRF algorithm to form a Crypto Random Verification Agent, with a threshold of M (default threshold is 9 of 15, set by the agent creator as a fault-tolerant parameter).
- Each TEE node remains unaware of its agent assignment or the presence of other members within the same agent, preventing collusion among nodes and making targeted attacks unfeasible, achieved through Ring VRF algorithm.
- Ring VRF algorithm, built upon ZKP and VRF, elects agent members where each agent generates a virtual key and a collective account address using Multi-Party Computation (MPC).
- In case a few TEE nodes go offline or crash, the system promptly introduces a corresponding number of new nodes, creating new key shares via a key handover protocol (previous key shares are systematically eliminated).
- Even if all N nodes within an agent are functioning properly, the system periodically reselects N nodes to maintain the original agent, further enhancing security.
- TEE nodes store key shares and execute core codes including Ring VRF, MPC, and other essential peripheral programs, such as light nodes.

In essence, through the Crypto Random Verification Agent mechanism, DeepSafe constructs an impenetrable black box. If a TEE node is operational, no entity, including the node operator, other nodes, or external attackers, can discern its operational status, its associated CRVA, other nodes within the same CRVA, the consensus communications, or the signed messages. Under this premise of"unawareness" and"self-unawareness", as long as DeepSafe itself remains secure, each dynamic hidden member is secure. To ensure a high probability of a successful attack, an attacker must control the majority of nodes in DeepSafe. However, as the programs operating within the TEE are immutable, attackers can only cause network downtime without seizing assets within the network.

3.3.2 Data availability layer

The Data Availability (DA) Layer refers to the state of DeepSafe ensuring that transactional data from both Bitcoin and the layer 2 networks is accessible and verifiable by all nodes within the network. In the context of DeepSafe, data availability is a crucial aspect, ensuring that every node can access submitted transactions and block data. If data is unavailable, other nodes cannot verify transactions, potentially leading to network inconsistencies and insecurities.

The data availability Layer stands as a critical component within DeepSafe, responsible for managing and providing transactional data from all chains across the entire Bitcoin and layer 2 networks. When execution layers, such as Rollups, generate new transactions, this transactional data is submitted to DeepSafe's DA layer, ensuring that other chains and nodes can access this data. This shared data availability method facilitates interconnections between various chains, enabling them to share security.

DeepSafe's implementation of data availability (DA) utilizes Merkle trees and hash functions to create immutable digests of the data. This enables nodes to verify if the received data matches the submitted data by comparing the digests.

Overall, data availability stands as a crucial component ensuring the consistency and security of the entire Bitcoin ecosystem, particularly within a modular stack, providing a shared security foundation for various layers.

3.3.3 Forced Exit and Escape Hatch

The Forced Exit and Escape Hatch within Bitcoin's Layer 2 Rollup are two critical concepts that need consideration in the design of DeepSafe's verification layer. Both aim to ensure the security of user assets

in cases of network issues or misuse.

1. Forced Exit

   - **Definition**: Forced exit refers to situations where the network permits users to extract their assets from Layer 2 to Layer 1, namely the Bitcoin network.
   - **Scenario**: Forced exit allows users to swiftly exit Layer 2 and retrieve their assets in case of network errors, malicious activities, or other emergencies.
   - **Implementation**: The forced exit in DeepSafe is facilitated through Crypto Random Verification Agents, the data availability layer, and smart contracts. Contracts can be triggered to enable users to withdraw their assets.

2. Escape Hatch

   - **Definition**: An escape hatch is a security mechanism allowing network administrators or contract creators to intervene and potentially shut down the Layer 2 network when necessary.
   - **Scenario**: The escape hatch permits intervention by relevant parties when significant vulnerabilities, malicious activities, or other threats are detected within the network. It enables the suspension of network activity and the implementation of necessary measures, such as contract closure or fund freezing.
   - **Implementation**: An escape hatch typically involves multi-party involvement and multiple signatures (CRVA) to ensure its legitimate use. This might require alignment with the governance structure of the network community.

In designing the functionalities of the escape hatch, a critical consideration arises: How can assets be retrieved back to the user's Bitcoin account when all nodes in the verification network are non-functional? To tackle this, we propose utilizing Bitcoin's Taproot feature and time-lock mechanisms. By integrating OP_CHECKLOCKTIMEVERIFY or OP_CHECKSEQUENCEVERIFY operations within the script, we enable 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 CRVA's signatures within this period. In an extremely unlikely scenario of substantial loss of private key shares managed by the CRVA during this period, asset retrieval remains possible upon the time lock expiration, enabling retrieval from a collectively managed account.

3.4 Governance Framework

The governance framework of DeepSafe is divided into specific applications and layers to ensure non-overlapping governance across its components. Drawing inspiration from Polkadot, its governance mechanism employs a consensus mechanism known as"Nominated Proof-of-Stake" (NPoS) [6], relying on the voting of token community members. Here are the primary governance mechanisms of DeepSafe:

1. **Nominated Proof-of-Stake**: DeepSafe utilizes NPoS as its consensus mechanism, allowing $\$DEF$ token holders to select validators through voting. These validators are responsible for block generation and maintaining network security. NPoS aims to enable $\$DEF$ token holders to participate in network governance and ensure security.

2. **Governance participation**: $\$DEF$ token holders play a crucial role in governance by expressing their opinions on network protocols and parameters through voting. Holders with more DST tokens possess greater voting power in governance.

[6] NPoS election algorithms, https://wiki.polkadot.network/docs/learn-phragmen

3. **Proposal and voting**: All $\$DEF$ token holders can propose governance changes covering various aspects such as protocol upgrades, parameter adjustments, and introducing new features. Governance proposals require majority consent through the voting process to take effect.

4. **Council**: DeepSafe has a council elected by token holders. The council plays a crucial role in governance decisions by supporting or vetoing governance proposals. Its existence aims to ensure rational and efficient decision-making.

5. **Public engagement**: DeepSafe emphasizes community involvement. Through transparent proposal and voting procedures, community members have the opportunity to participate in network development and express opinions.

The governance framework adopted by DeepSafe is open and community-driven, aiming to maintain decentralization and inclusivity within the network. This mechanism enables the network to adapt flexibly to diverse developmental needs and allows community members to voice opinions on the network's future direction.

4 Key Features

4.1 DeepSafe Stack

DeepSafe Stack is a universal development stack for building the L2 blockchain ecosystem, aimed at driving the development of DeepSafe and the Bitcoin ecosystem. DeepSafe Stack can be seen as a collection of software components maintained by the core development team of DeepSafe, where some components help define new layers of the stack, while others exist as embedded modules within the stack [7].

For DeepSafe, securely creating new chains within the Bitcoin ecosystem that can interoperate becomes increasingly crucial. Therefore, the primary focus of DeepSafe Stack is to create a shared, high-quality, and fully open-source system for establishing new L2 blockchains. By collaborating on shared standards, the core team of DeepSafe can avoid repeatedly building similar software in isolated environments.

DeepSafe Stack can be seen as software components defining specific layers of DeepSafe ecosystem or embedded as modules within existing layers. While the current core of DeepSafe Stack is infrastructure for running L2 blockchains, theoretically, it encompasses various layers above the underlying blockchain, including block explorers, messaging mechanisms, governance systems, and other tools.

4.1.1 Execution layer (EVM)

The execution layer defines the structure of the state within DeepSafe Stack system and specifies that changes in this state are governed by state transition functions. When a derived layer receives input through the engine API, it triggers state transitions. The abstraction of the execution layer allows for modifications to the VM or the use of an entirely different underlying virtual machine.

The Ethereum Virtual Machine (EVM) has undergone several years of development, and its entire developer ecosystem is well-established and widely accepted. It is the first execution layer engine module supported by DeepSafe, using the same state representation and state transition functions as the Ethereum Virtual Machine. In the Ethereum Rollup configuration within DeepSafe Stack, the EVM module is a slightly modified version of the EVM, adding support for L2 transactions initiated on Bitcoin and including additional L1 data fees for each transaction to consider the cost of publishing transactions to the Bitcoin network.

[7] The layers at the bottom of the stack are typically more strictly defined (such as the data availability layer), while the layers at the top of the stack (such as the governance layer) become more abstract.

4.1.2 Interoperability within Bitcoin

Through the interoperability protocol constructed by the Crypto Random Verification Agents within DeepSafe, from a security perspective, it prevents external hacking attacks while also avoiding internal collusion. In terms of performance and user experience, DeepSafe's cross-chain experience matches that of external verification bridges without making any sacrifices. It not only resolves the"impossible triangle" problem in cross-chain regarding security, generality, and scalability but also achieves optimal levels in terms of cost, speed, and availability.

- **Cost**: The primary cross-chain cost lies in the on-chain gas cost, where DeepSafe's cost for verifying a cross-chain message is only equivalent to the cost of a single signature verification, matching that of an external verification bridge.
- **Speed**: Here, we solely evaluate the latency of cross-chain bridges without considering the finality of the chains. Due to the absence of additional on-chain and off-chain computations and the relay chain design (which might lead to redundant secondary verifications), DeepSafe's cross-chain speed can reach its maximum level.
- **Security**: As discussed previously, DeepSafe is equipped to thwart external attacks and internal collusion.
- **Availability**: To put it simply, it prevents downtime. Each CRVA within DeepSafe is equipped with one or multiple backup CRVAs during creation, addressing availability issues caused by more than half of the TEE nodes being offline.
- **Generality**: Supporting asset and arbitrary message cross-chain functionalities, DeepSafe meets the aforementioned requirements.
- **Scalability**: Swiftly supporting new chains. DeepSafe only requires deploying a set of simple contracts to support a new chain and currently supports all mainstream blockchains. Moreover, DeepSafe is not limited by the Turing completeness of chains and can support non-Turing complete chains like BTC without introducing new trust assumptions.

4.2 Security and Decentralization

The assurance of security and decentralization stands as a cornerstone within the Bitcoin ecosystem, serving as the primary design objective for DeepSafe. This directly encompasses user trust, the security of digital assets, resistance to censorship, individual privacy, the reliability of smart contracts, and the stability of the entire blockchain network. Thus, ensuring the security of DeepSafe system is a crucial factor in fostering its widespread adoption and development.

The pursuit of security within DeepSafe not only involves technical considerations but also embodies an ideological exploration of societal and human relationships. It reflects a desire for decentralization, liberty, and fairness, aiming to construct a more equitable and trusted social structure.

As a verification layer for Bitcoin, DeepSafe is dedicated to two security assurance aspects within the entire ecosystem: the network security of the Bitcoin verification layer and the shared security of Bitcoin Layer 2, with the security of the verification layer forming the foundation.

4.2.1 Verification layer security

DeepSafe focuses on addressing the decentralization and security concerns surrounding signature verification. While public blockchains like Bitcoin and Ethereum offer sufficient decentralization and security, many associated tools operate in a relatively centralized manner. For instance, issues of security have

been prevalent in cross-chain functionalities, wallets, centralized exchanges, oracle services, and centralized asset custody. These problems stem from the foundational implementation layer, where a genuinely decentralized yet secure distributed signature verification management solution is lacking.

Innovatively, DeepSafe addresses this challenge using MPC (Multi-Party Computation), ZKP (Zero-Knowledge Proof), and TEE (Trusted Execution Environment) technologies. By employing mathematical methods rather than centralized authority, DeepSafe injects a foundational layer of trust into the entire blockchain industry. While maintaining the Bitcoin consensus layer rules unchanged, the Bitcoin verification layer built on DeepSafe inherently possesses decentralized and secure characteristics, achieving a level of security equivalent to Bitcoin. Further implementation details can be referenced in DeepSafe's technical paper [17].

4.2.2 Shared L2 security

In a singular blockchain, security assurances for all users, applications, and Rollups stem from the foundational layer. DeepSafe, functioning as the Bitcoin verification layer, ensures security for the Layer 2 networks it serves through the Bitcoin verification layer's Crypto Random Verification Agent (CRVA) and Data Availability (DA).

DeepSafe offers the fundamental functionalities necessary to establish cross-chain security, namely Crypto Random Verification Agents and Data Availability. On one side, this is because every layer utilizing DeepSafe needs to store all transactional data in the Data Availability layer to prove its availability. On the other hand, layers using DeepSafe manage assets on Bitcoin through Crypto Random Verification Agents. This means chains can effortlessly connect, monitor, and interoperate. With the inherent security of the underlying Crypto Random Verification Agent (CRVA) and DA layer, hard forks and soft forks also become remarkably more accessible.

Simultaneously, DeepSafe allows parallel experimentation with various experimental execution layers, even without dependency on the settlement layer, yet still benefitting from shared data availability and the advantages of Crypto Random Verification Agents. This implies a potentially proportional increase in iteration speed to the number of users. Over time, this fosters compound improvements in execution layers because DeepSafe isn't confined by a singular entity with a centralized execution layer. The execution, data availability, and verification layers are decoupled. The modular and permissionless nature allows for experimentation, providing developers with flexible choices.

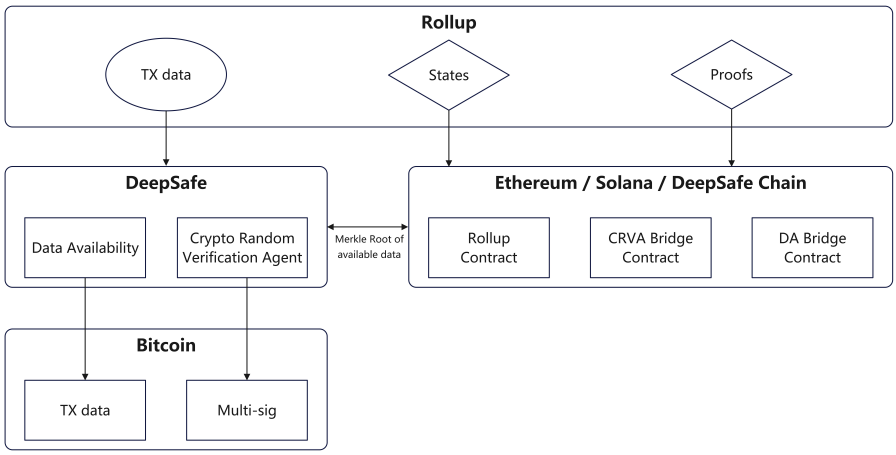

Figure 4: Shared Layer 2 Security via DeepSafe.

5 Use Cases

5.1 Decentralized BRC-20 Indexer

BRC-20 stands as one of the most significant innovations in the Bitcoin ecosystem in recent years, amplifying ecosystem diversity while notably benefiting miners within the network. However, the existing BRC-20 indexing mechanism suffers from inadequate transparency and a relatively high level of centralization, deviating from the foundational principles of the industry.

With DeepSafe, there emerges the possibility of establishing a decentralized BRC-20 indexer. This indexer could sort BRC-20 protocol operations in a chronological sequence, presenting a secure, transparent, and trustworthy indexing functionality. Key attributes include tamper resistance, resistance to censorship, and leveraging the Bitcoin chain as the singular trusted data source, thus eradicating dependency on singular, centralized, off-chain indexers.

Outlined in Figure 5 is the technical architecture[8] for constructing such a decentralized indexer using DeepSafe.

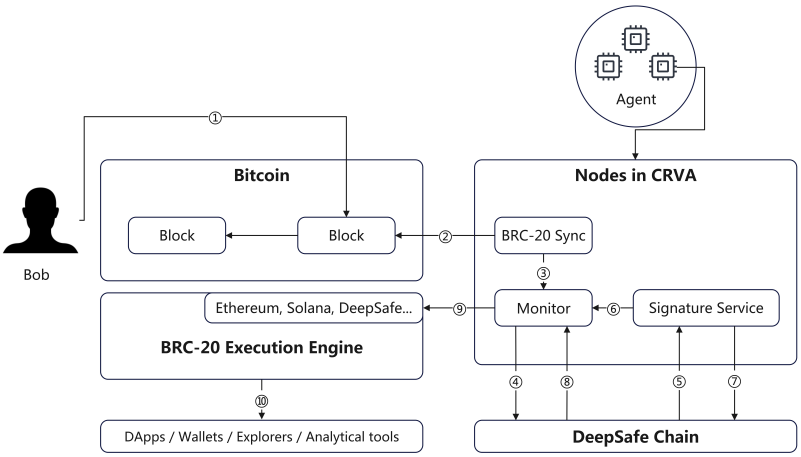

Figure 5: A decentralized BRC-20 indexer through DeepSafe.

1. Bob initiates a BRC-20 inscription (e.g., deploy, mint, transfer).
2. BRC-20 Sync service indexes BRC-20 inscriptions within Bitcoin blocks.
3. BRC-20 Sync pushes the set of valid operations to the monitor.
4. The monitor module submits the set of valid operations along with corresponding Bitcoin block heights to DeepSafe Chain.
5. DeepSafe Chain triggers the"pending verification of operations" event.
6. All CRVAs in the network examine the legitimacy of this operation set.
7. Post-consensus among the CRVAs, the signed result is submitted to DeepSafe Chain.
8. DeepSafe Chain triggers the"operations verified" event.
9. Monitor submits this event to BRC-20 Execution Engine, which can be any sovereign blockchain such as Ethereum, Solana, or DeepSafe Chain.
10. Post this process, the indexing related to BRC-20 is stored on any sovereign blockchain, available for third-party use and verification, such as DApps, wallets, explorers, analytical tools, and more.

[8]The numbers in the diagram represent the sequence of indexing.

5.2 Omnichain Operable Token Discipline

Through DeepSafe, we introduce another prospective use case - ZeroOne: An omnichain operable token discipline. This protocol enables asset issuance on the Bitcoin chain and the operation of assets on its Layer 2, creating a comprehensive framework for interchangeable tokens. Differing from existing protocols like BRC-20, ZeroOne is UTXO-based, allowing seamless integration with Bitcoin's existing architecture while minimizing redundant outputs. ZeroOne distinctly represents balances stored within UTXO.

Transactions involving ZeroOne contain specific protocol messages, initiated through OP_RETURN outputs along with additional data pushes. Additionally, assets issued via ZeroOne on Bitcoin can be seamlessly transferred to Layer 2 networks through predefined cross-chain instructions. Furthermore, ZeroOne allows for the inclusion of specific human-readable symbols and decimal configurations.

In summary, ZeroOne presents a simplified and more intuitive approach to asset issuance on Bitcoin and the operation of interchangeable tokens on its Layer 2. Figure 6 illustrates the overall process of the Omnichain Interoperable Token Protocol built on DeepSafe.

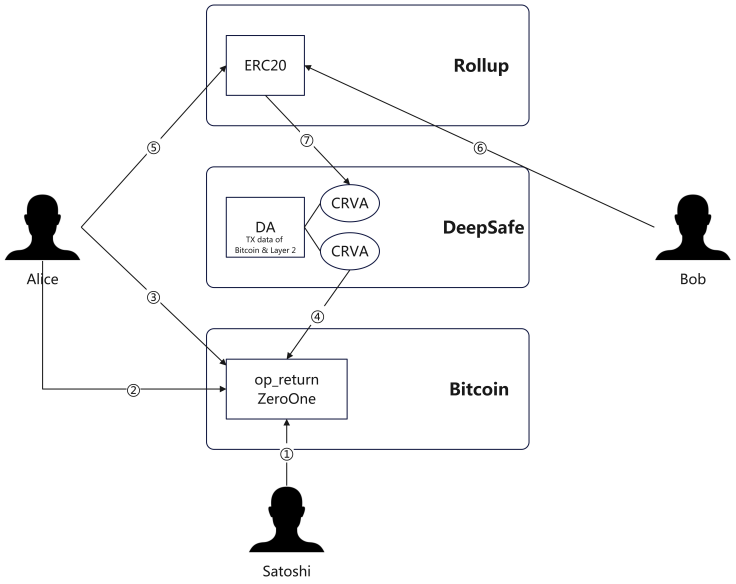

Figure 6: An omnichain operable token discipline through DeepSafe.

1. Satoshi issued 1000 USDT based on the ZeroOne protocol; the ledger data of the issuance is synchronized through CRVA to the DA layer of DeepSafe.

2. Alice minted 500 USDT; the corresponding ledger data will be synchronized through CRVA to the DA layer of DeepSafe.

3. Alice transferred 300 USDT to the Layer 2 network through cross-chain instructions, leaving 200 USDT on the Bitcoin mainnet.

4. CRVA synchronized the Bitcoin ledger data and detected the operation in 3; subsequently, CRVA will mint 300 USDT to Alice's account in the Layer 2 network.

5. Alice transferred 100 USDT of her own in the Layer 2 network to Bob; the corresponding ledger data will be synchronized to the DA layer of DeepSafe.

6. Bob transferred 100 USDT from his own in the Layer 2 network to 50 USDT in the Layer 1 network through cross-chain instructions.

7. CRVA synchronized the Layer 2 ledger data and detected the operation in step 6; consequently, CRVA will mint 50 USDT to Bob's account on the Bitcoin network.

6 Conclusion

The evolution of Bitcoin and subsequent endeavors to enrich its capabilities laid the groundwork for Ordinals protocol and the ensuing BRC-20 innovation, showcasing the potential for asset issuance and diverse functionalities within the Bitcoin framework. However, the Bitcoin ecosystem faced challenges in achieving broader use cases and scalability improvements.

DeepSafe emerges as a promising solution, leveraging advanced cryptographic tools and components to enhance Bitcoin's scalability, security, and cross-chain capabilities. This paper proposed a programmable framework with a"state + computation + verification" mechanism, aimed at providing convenience for building Bitcoin Layer 2 on DeepSafe for all blockchains and establishing a strong foundation for cross-chain experiences, secure asset issuance, and verification layer security.

By constructing a robust decentralized verification network, DeepSafe achieves secure and decentralized scalability for Bitcoin without altering its consensus rules. Technological innovation and component-based design offer developers and existing blockchain networks a multi-layered stack (DeepSafe Stack), supporting the rapid and secure construction of Bitcoin L2 while enabling interoperability with other ecosystems. Through the NPoS consensus mechanism and governance architecture, DeepSafe relies on community engagement to drive network development, ensuring decentralized decision-making and governance.

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 Gün 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] Domo. brc-20 experiment, 2023.

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

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

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

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

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

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

[17] Zeyuan Yin, Bingsheng Zhang, Jingzhong Xu, Kaiyu Lu, and Kui Ren. Bool network: An open, distributed, secure cross-chain notary platform. *IEEE Transactions on Information Forensics and Security*, 17:3465–3478, 2022.