Alison - A zkEVM Rollup for Bitcoin

Abstract

Alison is a collaborative initiative between Bison Labs and XLink, focused on developing a zero-knowledge Ethereum Virtual Machine (zkEVM) rollup for Bitcoin. This innovative solution aims to enhance the Bitcoin ecosystem by enabling scalable, decentralized computation and smart contracts while addressing liquidity fragmentation issues inherent in the current Bitcoin landscape. By leveraging cutting-edge technologies, Alison seeks to empower developers and users alike to explore new decentralized applications (dApps) on Bitcoin.

Introduction

Background

The introduction of smart contracts, primarily through the Ethereum blockchain, has been pivotal in supporting diverse applications including decentralized finance (DeFi), non-fungible tokens (NFTs), and gaming. These smart contracts have significantly contributed to the development and prominence of the Web3 ecosystem. Conversely, Bitcoin, the highest-valued cryptocurrency globally, has been predominantly recognized for its stability, security, and decentralization, focusing mainly on value storage and straightforward transaction processing.

However, the evolving perspective within the Bitcoin community highlights the need for broader functionalities beyond being merely "digital gold." The integration of smart contract capabilities and liquidity connectivity can facilitate the Bitcoin network in supporting dApps, sophisticated financial protocols, and automated contract executions. This transformation will invigorate the Bitcoin ecosystem, attracting more developers, investors, and users.

The implementation of smart contracts and composable liquidity on Bitcoin can significantly improve its functionality, scalability, and user experience. By utilizing Layer-2 (L2) solutions and other technological advancements, Bitcoin can transition into a more comprehensive blockchain platform while maintaining security and decentralization.

Challenges

The primary challenges facing Bitcoin's expansion into more complex applications include:

- **Lack of Full Smart Contract Support**: The inherent limitation of the Bitcoin blockchain lies in its lack of Turing completeness, preventing it from directly supporting the execution of complex smart contracts. Consequently, numerous startup teams are investigating Bitcoin L2 solutions to expand its functionality.
- **Liquidity Fragmentation**: The diversity within the Bitcoin ecosystem results in fragmented liquidity. This fragmentation complicates user interactions and increases barriers to entry for decentralized applications.
- **Existing Alternatives**: Current alternatives to centralized off-chain computation are either equally expensive or lack a strong connection to Bitcoin's security model.

Alison's Solution

Alison addresses these challenges by providing a cost-effective zkEVM-based rollup secured with Bitcoin. This solution integrates smart contract functionality and liquidity connectivity, thus enhancing user experience and fostering broader adoption of DeFi on Bitcoin.

Bison Network: A Bitcoin Layer-2 Scaling Solution

To preserve the decentralization of the Bitcoin network while ensuring security and enhancing real-world applicability, Bison Network was developed as a sovereign rollup utilizing Zero-Knowledge Scalable Transparent Arguments of Knowledge (ZK-STARK). By leveraging zero-knowledge technology and using Bitcoin as its Data Availability (DA) layer, Bison Network roots its security deeply within the Bitcoin network.

Architecture Overview

The architecture of Bison Network presents a comprehensive scaling solution that enhances both on-chain and off-chain operations through integration with ZK-STARK technology. The solution is divided into two main segments: on-chain verification and off-chain execution.

1. **Off-chain Execution Layer**:
    - **Execution Layer**: Responsible for processing messages, executing smart contracts, and generating zero-knowledge proofs (ZKPs) to verify correctness.
    - **Rollup Layer**: Enhances scalability by batch-processing numerous transactions into a single block submitted to the main chain.

    When a transaction is initiated by users:

    - The sequencer retrieves messages from a pending queue.
    - It creates a RISC Zero environment that integrates with a RISC-V Ethereum Virtual Machine (rEVM), establishing the Zero-Knowledge Ethereum Virtual Machine (zkEVM).
    - The zkEVM collects necessary data such as account states and smart contract bytecode to execute within this virtual machine.
    - After processing transactions, it generates a new state along with ZKPs certifying execution correctness.
2. **On-chain Verification Layer**:
    - Inscribes ZKPs onto the Bitcoin blockchain for verification by network participants.
    - Ensures that all state transitions are valid and trustworthy through state proofs.
    - Incorporates a data availability adapter that guarantees transaction data is readily available for verification.

RISC Zero

The RISC Zero Zero-Knowledge Virtual Machine (zkVM) enables Bison Network to verify correct execution of Rust code efficiently. It allows developers to leverage existing Rust packages to build verifiable software applications quickly. The core process involves compiling guest programs into an Executable and Linkable Format (ELF) binary which is then executed within the zkVM environment.

REVM

REVM is an Ethereum Virtual Machine (EVM) implementation written in Rust that focuses on speed and simplicity. It successfully passes all Ethereum test suites ensuring reliability while being compatible with Solidity programs. By integrating REVM within RISC Zero's environment, Bison Network enhances security through zero-knowledge proofs for each transaction executed.

XLink: The Liquidity Layer

XLink enhances Bitcoin's integration into DeFi by providing seamless cross-chain transactions through

an innovative "liquidity layer" designed specifically for this purpose.

Architecture

1. **Intent-Based Routing Engine**:
   - This core component enhances interoperability between different blockchain networks.
   - It dynamically routes liquidity based on user intent, simplifying complex transaction processes.
   - Users can specify desired outcomes without needing to manage intricate transaction details manually.
2. **Direct Bitcoin Event Validation**:
   - XLink validates events directly within its framework rather than relying on external validators or complex processes.
   - This mechanism reduces risks associated with traditional bridging solutions while aligning with Bitcoin's characteristics.
3. **Decentralized Validator Network**:
   - Monitors asset transfers between non-Bitcoin networks using a decentralized network of validators integrated with a cross-chain messaging layer known as Bitcoin Oracle.
   - Ensures accuracy during transactions by producing cryptographic proofs before assets are sent to relevant addresses.
4. **Institutional-grade Multi-Party Computation (MPC) Wallets**:
   - Users interact with MPC wallets that require multiple signatures for transaction approvals.
   - This method enhances security by ensuring private keys are never fully assembled in one location.

Conclusion

Alison represents a significant advancement in integrating Bitcoin with decentralized finance by addressing key challenges related to smart contract support and liquidity fragmentation. By combining the respective expertise of Bison Labs and XLink, Alison simplifies user experiences, enhances interoperability, and unlocks new opportunities for Bitcoin holders in the DeFi landscape while maintaining security and efficiency.

With its robust architecture and innovative solutions, Alison is poised to broaden Bitcoin's role within the broader blockchain ecosystem significantly. This initiative not only addresses existing pain points but also sets a foundation for future developments in the rapidly evolving landscape of blockchain technology.

Brief History of Bison Network

Bison Labs emerged as a significant player in the Bitcoin ecosystem with a vision to enhance its scalability and functionality through Layer-2 solutions. Launched in March 2024 on testnet, Bison Labs utilizes Zero-Knowledge Scalable Transparent Arguments of Knowledge (ZK-STARK) technology to create sovereign rollups that improve transaction efficiency while enabling smart contract capabilities on Bitcoin.

The platform leverages the Ordinals protocol as its data layer, allowing rollup proofs and network statuses to be inscribed directly onto the Bitcoin blockchain. This integration not only ensures immutability but also enhances transparency within the network. In March 2024, Bison Labs successfully closed a pre-seed funding round led by Portal Ventures with participation from several notable investors including UTXO and Waterdrip Capital.

Bison Labs aims to empower developers by providing robust tools for building decentralized applications (dApps) secured by Bitcoin's foundational layer. As it continues to develop its infrastructure, Bison Labs is poised to play a crucial role in expanding DeFi opportunities within the Bitcoin ecosystem.

Brief History of XLink

XLink was launched in December 2023 as a pioneering intent-based omnichain liquidity network designed

specifically for Bitcoin. Initially known as the ALEX Bridge, XLink transitioned into an independent entity following a governance proposal backed by $ALEX token holders who recognized the need for dedicated governance over bridging operations.

The platform focuses on simplifying cross-chain interactions between Bitcoin and Ethereum's DeFi ecosystem while offering a "native-like" experience for BTC holders. By abstracting complexities between Layer 1 (L1) and Layer 2 (L2) protocols, XLink allows users to interact with L2 smart contracts using native BTC without needing complex wrapping processes.

XLink employs an intent-based routing engine that dynamically routes liquidity based on user goals, enhancing efficiency in asset transfers and interactions with decentralized finance applications. The platform also integrates advanced security measures through partnerships with leading custody solutions like Cobo and Coincover to ensure robust protection against hacking and operational disruptions.

As XLink continues to evolve, it is committed to reshaping financial interactions within the DeFi landscape by making them more accessible and secure for users globally.

Website and Social Media Details

Bison Network

- **Website**: https://www.bisonlabs.io
- **Twitter**: @BisonLabs
- **Discord**: https://discord.gg/bisonlabs
- **GitHub**: https://github.com/BisonLabs

XLink

- **Website**: https://www.xlink.network
- **Twitter**: @XLinkNetwork
- **Discord**: https://discord.gg/xlinknetwork
- **GitHub**: https://github.com/XLinkNetwork