XLink: The Liquidity Layer on Bitcoin*

October 1, 2024

Abstract

XLink is an innovative "liquidity layer" on Bitcoin, designed to enhance the integration of Bitcoin into the decentralized finance (DeFi) ecosystem. By providing the infrastructure to create seamless cross-chain transactions on Bitcoin, XLink aims to help builders empower BTC holders to utilize their assets, using a Bitcoin wallet only, across Bitcoin ecosystem without the complexities typically associated with such interactions. This white paper outlines the architecture, core components, features and use cases of XLink.

Introduction

Background

Bitcoin [4] , the pioneering cryptocurrency, has established itself as a store of value and a medium of exchange. However, its limited smart contract capabilities and interoperability with other blockchain networks have restricted its full potential in the rapidly evolving DeFi landscape. As DeFi continues to grow, there is an increasing demand for solutions that allow Bitcoin holders to leverage their assets in a broader range of financial applications.

Problem Statement

Bitcoin holders face several challenges when attempting to engage with DeFi platforms, due mainly to Bitcoin's limited smart contract capabilities. This is well known and has been discussed both in academia and by practitioners. For example, [3, 1] discuss the limitations of Bitcoin's scripting language, which lacks support for complex transactions and advanced logic like loops and conditional statements. These limitations hinder Bitcoin's ability to fully participate in DeFi applications, which often require more sophisticated smart contract functionality.

In practice, such limitation leads to poor user experience with, among others, the need for wrapping/unwrapping BTC, multiple transactions required to complete a cross-chain transaction, and which may introduce centralization, increasing vulnerability.

XLink Solution

XLink addresses these challenges by offering an infrastructure that facilitates direct interactions between Bitcoin and various blockchain ecosystems using a Bitcoin wallet only. By leveraging advanced technologies, XLink aims to help builders empower BTC holders to utilize their assets across Bitcoin ecosystem without the complexities typically associated with cross-chain transactions. We call this approach "Bitcoin-Centric Chain Abstraction".

Bitcoin-Centric Chain Abstraction

Bitcoin-centric chain abstraction refers to the development of frameworks and protocols that enable seamless interactions and interoperability between Bitcoin and other blockchain networks while simplifying the user experience. This approach aims to eliminate the complexities associated with managing multiple blockchains, allowing users to engage with

*https://www.xlink.network

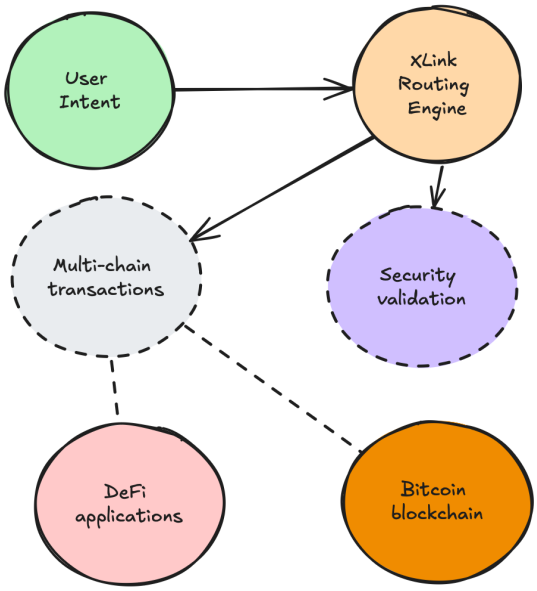

Figure 0.1: XLink Intent-based Routing Engine

decentralized applications (dApps) and services without needing extensive technical knowledge or multiple wallets.

Bitcoin-centric chain abstraction, therefore, focuses on creating a user-friendly interface for Bitcoin holders that hides the underlying complexities of interacting with various blockchains. Bitcoin users can, using Bitcoin wallet only, perform transactions, access DeFi services, and manage assets across different networks without worrying about the specific technical details of each blockchain. By enabling Bitcoin to interact seamlessly with other blockchains (such as Ethereum), Bitcoin-centric chain abstraction enhances the overall functionality of Bitcoin within the broader decentralized finance (DeFi) ecosystem. This interoperability allows Bitcoin holders to leverage Bitcoin's liquidity while accessing a wider range of financial services.

XLink Architecture

Intent-based Routing Engine

The Intent-Based Routing Engine is a core component of XLink's architecture, designed to enhance the interoperability and efficiency of Bitcoin transactions across various blockchain ecosystems.

Intent-based routing [2] is a transformative approach in blockchain technology that enhances interoperability between different blockchain networks, allowing users to express their desired actions (or intents) without needing to understand the underlying complexities of each blockchain.

XLink's intent-based routing engine dynamically routes Bitcoin liquidity based on user intent, allowing for efficient asset transfers and interactions with decentralized finance (DeFi) applications. By focusing on user goals, the engine simplifies complex transaction processes. Users can specify their desired outcomes without needing to understand the intricate details of each transaction.

There are multiple benefits to this approach. XLink automates the translation of user intents into executable workflows. This reduces the likelihood of manual errors and enhances the efficiency of cross-chain interactions. For instance, if a user wants to stake assets on a different blockchain, the intent-based system can automatically handle the necessary steps—such as bridging assets and executing trades—without requiring users to manage each individual transaction. Further, the engine treats cross-chain operations as atomic, ensuring that all parts of a transaction either complete successfully together or not at all. This prevents inconsistent states across different blockchains and enhances overall security.

Direct Event Validation

Direct Event Validation is a key feature of the XLink architecture that enhances the security and reliability of transactions involving Bitcoin. This mechanism significantly differs from traditional bridging solutions, which often rely on external validators or complex processes to confirm transactions.

XLink operates by directly validating Bitcoin

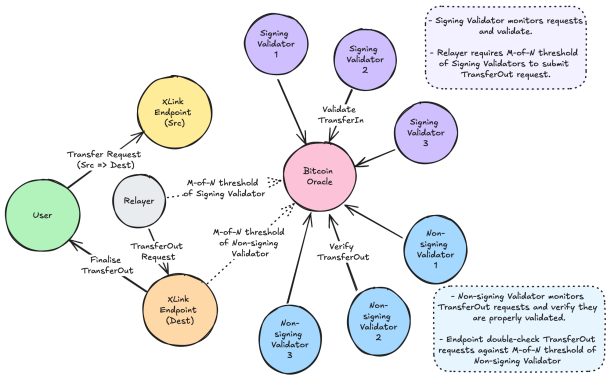

Figure 0.2: XLink Validator Network

events within its own framework [5]. This means that instead of depending on third-party validators or off-chain mechanisms, XLink confirms transactions natively on the Bitcoin network.

By validating events directly, XLink reduces the risk of errors and external manipulations that can occur in traditional bridging systems. This enhances the overall security of transactions, making them more robust and reliable.

Traditional bridges often experience delays due to lengthy confirmation processes. XLink's direct validation allows for quicker transaction finalization, which is crucial for better user experience. At the same time, the validation process aligns with Bitcoin's inherent characteristics, helping to mitigate risks related to blockchain reorganizations (reorgs). This alignment ensures that transactions remain valid even in the event of network fluctuations.

Decentralized Validator Network

Asset transfers between non-Bitcoin networks are monitored by a decentralized network of validators, through XLink's integration of Bitcoin Oracle, who produce cryptographic proofs to ensure accuracy and integrity during transactions. A minimum threshold of confirmations is required before assets are sent to the relevant address, enhancing trust in the system.

Bitcoin Oracle is a cross-chain messaging and consensus layer, developed by ALEX, for off-chain computation engines that builds on Bitcoin. Bitcoin Oracle provides infrastructure that allows two or more off-chain computation engines on Bitcoin to exchange messages, and provides the consensus model to validate such cross-chain messages.

When Xlink identifies a particular cross-chain transfer to process, it pulls the relevant consensus data from Bitcoin Oracle, verify them using its smart contract before processing them on the relevant destination chain.

XLink incorporates a mixture of signing and non-signing validators to secure its infrastructure, where the consensus (100% threshold) of the signing validators must be met to validate the consensus (51% threshold) reached by all the validators.

This security model brings the multiple benefits. It lowers the barrier to entry to join the validator network, encouraging more members of its community to participate in securing the XLink infrastructure. Security budget is replaced with a set of signing validators, which essentially acts as the secondary check against the consensus derived from the network. Larger part of the incentives can be allocated to encouraging the community to join and actively participate in securing the network. 51% threshold and the lower barrier to entry to join the network means it is expensive for the signing validators to take over the validator network. Likewise, malicious actors cannot take over the validator network even if they own all non-signing validators unless they also take over every signing validators.

Institutional-grade Multi-Party Computation (MPC) Wallets

On the Bitcoin side, users interact with MPC wallets to lock assets for bridging. This approach increases security by requiring multiple signatures for transaction approvals.

MPC is a cryptographic method that allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. In the context of cryptocurrency wallets, this means that private keys are never fully assembled in one location. Instead of having a single private key, MPC wallets split the key into multiple shares distributed across

different servers or devices. Each share is independently generated and stored, ensuring that no single entity has access to the complete key.

XLink partners with Cobo and Fireblocks for MPC custody technology and Coincover for disaster recovery solutions. These partnerships provide advanced security management for digital assets, safeguarding against hacking, theft, and operational disruptions. These partnerships are part of XLink's strategy to expand its reach within the Bitcoin DeFi ecosystem. The combination of advanced security technologies with innovative liquidity solutions makes it possible for XLink to become a central liquidity hub for Bitcoin.

Endpoints on Layer 2s

On non-Bitcoin networks, users interact with "Endpoints" to receive assets that have been bridged from the Bitcoin blockchain. This allows for a smooth transition of assets between different layers, enhancing user experience.

An "endpoint" refers to a specific point within a blockchain bridge architecture that facilitates the transfer of assets and data between two distinct blockchain networks. It serves as a connection point where transactions can be initiated, validated, and executed across chains.

When users lock their Bitcoin assets for bridging on the Bitcoin network, they subsequently engage with these Endpoints on L2s to access their bridged assets. This process abstracts the complexities involved in cross-chain transactions.

Key Features

Native-like DeFi Experience on Bitcoin

The term "native-like DeFi experience" refers to the ability for Bitcoin holders to engage with decentralized finance (DeFi) applications in a manner that feels seamless and intuitive, similar to how users interact with native assets on other blockchain networks.

XLink allows Bitcoin holders to interact directly, using Bitcoin wallet only, with L2 smart contracts using native Bitcoin (BTC) or Layer 1 (L1) assets. This eliminates the need for complex wrapping processes that are common in other ecosystems, making it easier for users to engage in DeFi activities without losing their Bitcoin's fundamental properties.

This interaction is facilitated by seamless asset transfers between Bitcoin and various L2 protocols (including Bitcoin meta-protocols), allowing users to lock BTC in a secure multi-party computation wallet and mint corresponding assets on L2s. This capability ensures that users can move their assets fluidly across different layers while retaining access to Bitcoin's security.

Enhanced User Experience

By integrating the broad Bitcoin ecosystem, XLink significantly reduces transaction barriers associated with using Bitcoin in DeFi applications. This efficiency is crucial for making DeFi more accessible to a broader audience.

Traditional bridges often involve lengthy waiting periods for transaction finalization. XLink addresses this by rapidly validating Bitcoin events, which minimizes delays and enhances the overall user experience when conducting transactions.

Decentralized Governance

XLink is governed by the XLinkDAO, which was established to oversee its operations and ensure sustainable development. XLinkDAO allows stakeholders to participate in decision-making processes. This decentralized model ensures that the interests of the community are represented and that governance is not centralized in a single entity.

Collaboration with ALEX Lab Foundation

While XLink operates autonomously as a separate entity, it maintains a collaborative relationship with the ALEX Lab Foundation. This partnership ensures

that developments within XLink align with broader goals of enhancing the Bitcoin ecosystem.

Use Cases

DeFi Participation

With XLink, Bitcoin holders can engage in various DeFi activities. For example, users can lend their Bitcoin assets to earn interest or borrow against them for liquidity. Participants can also engage in yield farming by providing liquidity to DeFi protocols and earn rewards, leveraging their Bitcoin holdings more effectively. For those looking to trade, its partnership with XLink allows ALEX to build their next generation trading engine, efficiently swapping Bitcoin and the assets issued on its blockchain for assets native on other blockchains without the need for complex wrapping or unwrapping processes.

Asset Transfers across Bitcoin ecosystem

XLink enables direct asset transfers between Bitcoin and other blockchain networks, such as Core Chain and Ethereum. This functionality allows users to move their Bitcoin assets across different platforms effortlessly, enhancing liquidity and accessibility in the DeFi space.

Institutional Adoption Support

As traditional financial institutions increasingly enter the cryptocurrency space, XLink positions itself as a bridge that facilitates institutional participation in Bitcoin-based DeFi activities. By providing secure and efficient access to Bitcoin liquidity, XLink appeals to family offices, pension funds, and high-net-worth individuals looking to invest in Bitcoin.

Integration with Existing Ecosystems

XLink acts as a connector between different blockchain ecosystems, enhancing the overall functionality of platforms like Stacks and Core Chain. This integration fosters a more cohesive DeFi landscape where users can benefit from the strengths of multiple networks.

Facilitating Financial Inclusion

By lowering barriers to entry for using Bitcoin in DeFi applications, XLink promotes financial inclusion. Users can participate in decentralized finance without needing extensive technical knowledge or significant investments.

Conclusion

XLink represents a significant advancement in integrating Bitcoin with the DeFi ecosystem by addressing key challenges in cross-chain liquidity and transaction efficiency. By simplifying user experiences, enhancing interoperability, and enabling seamless cross-chain transactions, XLink aims to unlock new opportunities for Bitcoin holders in the decentralized finance landscape while maintaining security and efficiency.

With its innovative architecture and focus on user experience, XLink is poised to broaden Bitcoin's role within the broader blockchain ecosystem significantly and become a crucial infrastructure component for the future of decentralized finance.

References

[1] Maher Alharby and Aad van Moorsel. Blockchain-based smart contracts: A systematic mapping study. *Computer Science and Information Technology*, 2017.

[2] Rob Behnke. Intent-centric blockchain: Are intents the next big thing in web3? *https://www.halborn.com/blog/post/intent-centric-blockchain-are-intents-the-next-big-thing-in-web3*, 2024.

[3] Shafaq Naheed Khan, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud

Bani-Hani. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications*, 14(5):2901–2925, 2021.

[4] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[5] Stacks. Reading from bitcoin state. 2024.