CoinFabrik

Design Considerations

August, 2023

Introduction

CoinFabrik was recently commissioned to conduct a comprehensive security review on the design of the DLC.Link project - an innovative platform aiming to provide financial applications and services with safe access to Bitcoin collateral through Discreet Log Contracts (DLCs). This document presents our findings from this assessment, focusing on various aspects such as system architecture, threat modeling, implementation details, and potential vulnerabilities.

The DLC.Link project seeks to revolutionize the way Bitcoin is used in financial transactions by enabling simple smart contracts for locked BTC transfers between two parties. By leveraging DLCs, which are built on top of Schnorr signatures and offer significant advantages over traditional multisig setups, the project aims to provide increased security, privacy, scalability, and flexibility in Bitcoin-based financial applications.

In this report, we will first introduce the concept of DLCs and their relevance within the context of the DLC.Link project. We then proceed to analyze its system architecture, identifying key components such as the client libraries, server implementation, and user interfaces. Next, we delve into threat modeling exercises to identify potential attack vectors against the platform's design and implementation. Based on our findings, we provide recommendations for mitigating identified risks and improving overall security of the DLC.Link project.

Summary

Discreet Log Contracts (DLCs) are simple smart contracts for locked Bitcoin transactions between two parties. They provide enhanced security by allowing only pre-defined outcomes such as payments between the involved parties and preventing any malicious third party from accessing or manipulating the funds. With DLCs, users can securely escrow, prove reserves, and transfer Bitcoin based on external data sources without relying on bridges or custodians. DLC.Link aims to create a platform for financial applications and services to leverage Bitcoin collateral safely by providing:

1. A wallet integration library for popular third-party Bitcoin wallets;
2. Smart contract libraries in various languages and platforms, starting with Ethereum and Stacks;
3. An Attestor application run by third-party service providers to enhance security and resilience. Attestors verify the outcome of transactions and sign CETs (Contract Execution Transaction);

4. Stand-alone DLC enabled wallets on backend servers.

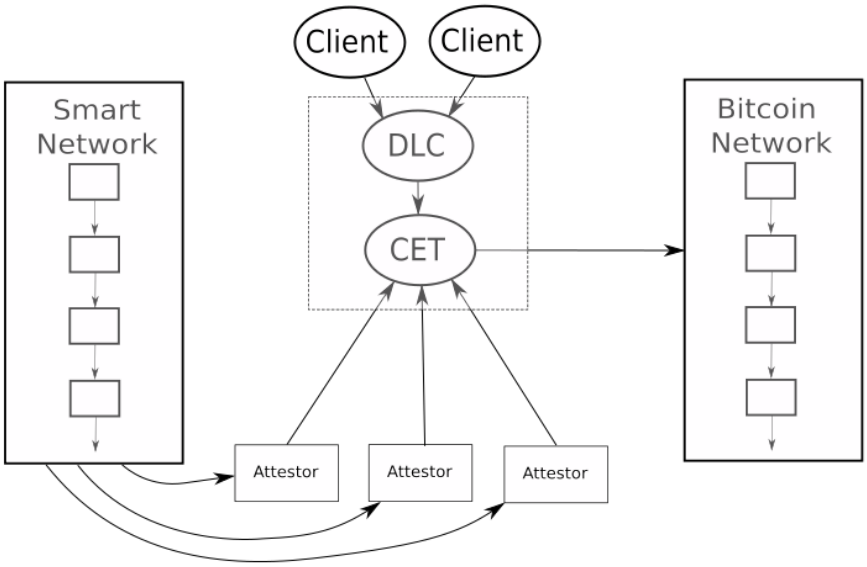

Image 1: Simplified diagram of the DLC.Link architecture.

Threat modeling

Threat modeling is the process of identifying potential security threats and vulnerabilities in a system. Based on the design, we identified possible threat models associated with this system:

Collusion between Participants and Attestors:
Threat: Borrowers or other participants could potentially collude with attestors to manipulate the outcomes of DLCs to their advantage.

Mitigation: Requiring a quorum of attestors to agree on an outcome can minimize this threat. Using multiple attestors to independently verify and attest to events adds another layer of security. Note: This is already implemented in the original design.

Misbehaving Attestors:
Threat: Attestors may behave maliciously, either due to incentives or technical issues, causing incorrect attestations or announcements.

Mitigation: Implementing a quorum requirement for attestations and using attestors from various organizations can mitigate the impact of misbehaving or malicious attestors. Monitoring tools like the Backchecker can help detect and remedy inconsistencies. Note: This is already implemented in the original design.

Key Management and Compromise:
Threat: Private keys used by attestors could be compromised, leading to unauthorized access and potential manipulation of DLC events.

Mitigation: Strict key management practices, like using Key Vaults, HSMs, regular key rotation, and secure storage, can mitigate the risk of key compromise. Keeping access to older keys until all attestations using that key are completed helps maintain the integrity of events.

Blockchain Listening Service Risks:
Threat: Services responsible for listening to the blockchain (like Infura or Stacks API) could face availability issues, leading to missed events or out-of-sync states.

Mitigation: Implementing a separate application like the Backchecker to query and verify past events can help ensure data consistency. Automatic remediation can be set up to address inconsistencies detected by the Backchecker.

Third-Party Deployment and Modification:
Threat: Third parties could deploy modified versions of the code, potentially compromising the security of the network.

Mitigation: Relying on a multi-node network and designing attestors to not directly benefit from altered outcomes can provide a level of security against modified code. Vigilant monitoring and reputation systems for third-party deployment can help mitigate this risk. Also, currently attestors are manually white-listed on the smart-contracts, but this functionality may change in the future.

Data Source Manipulation:
Threat: Manipulation of data sources used for attestation, such as smart contracts on other blockchain networks, could lead to incorrect outcomes.

Mitigation: Using trusted data sources and potentially cross-referencing information from multiple sources or Oracles can help mitigate the risk of data manipulation.

Backchecker and Attestor DoS:
Attack: Attackers overwhelm the Backchecker or Attestor components with a high volume of requests, preventing them from effectively monitoring and verifying events.

Impact: Reduced monitoring effectiveness, delayed detection of anomalies, potential incorrect event validation.

Mitigation: Implement rate limiting, prioritize critical requests, and use distributed monitoring mechanisms to distribute the load. Also DDOS protections like Cloudflare should be implemented in all critical internet-facing services.

Proposed Design Enhancements

Key management:
Proper key management is vital for maintaining the effectiveness of this security system. Keys are used by attestors to sign CETs. If these keys were compromised or mismanaged, it could lead to serious consequences such as unauthorized access to funds, and manipulation of DLCs. The preferred solution is to use Hardware Security Modules (HSMs). HSMs are physical devices that store cryptographic keys securely and provide controlled access to them when needed. They offer high levels of protection against both digital and physical attacks, making them ideal for storing sensitive information like private keys used by the attestors. Cloud services often provide well-documented APIs or command-line tools to access the HSMs, but being a recent technology, sometimes the APIs are development previews or are incomplete. A custom HSM like the Ledger platform is another option, with lower cost but bigger complexity as it requires custom development.

Recovery Mechanisms:
The system avoids single points of failure by using a quorum of attestors to validate transactions, but in the remote case that the quorum fails to reach an agreement, the DLC contracts can lock funds indefinitely. This can be avoided by

using standard recovery mechanisms used in the bitcoin network such as Bitcoin timelocks .

Monitoring system reliability:

The health monitor and Backchecker are two essential subsystems within the DLC-Link framework that provide a robust security mechanism for data integrity verification. While these systems do not have any capability to modify the system, they can still be vulnerable due to old or incorrect information caused by external system malfunctions or malicious attacks.

The health monitor is responsible for monitoring the overall health of the DLC-Link network and alerting users when issues arise. It periodically checks various parameters such as connectivity, performance metrics, and data consistency across different nodes in the network. This helps ensure that all components are functioning correctly and allows administrators to take corrective action if necessary. On the other hand, the Backchecker is designed to automatically verify the integrity of DLC transactions, and control the correct behavior of attestors, thus maintaining the trustworthiness of the entire system.

Although neither subsystem has direct control over modifying the DLC-Link network itself, they can still be susceptible to receiving outdated or incorrect information due to external factors. For example:

1) External System Malfunction: If an upstream system (I.E. Etherscan) feeding data into the modules experiences a failure, it may send corrupted or incomplete information which could lead to false positives in the health monitor and Backchecker reports, or worse, it can hide a malfunctioning system.

2) Malicious Attacks: Hackers might attempt to inject fake data into the network with the intention of causing disruptions or covering up their tracks after performing illicit activities.

3) Time Synchronization Issues: Misconfigured clocks on individual nodes can result in mismatched timestamps across different components of DLC-Link, leading to incorrect assessments by the health monitor and Backchecker about when certain events occurred, or even ignore warnings or malfunctions.

4) Human Error: Mistakes made during configuration or maintenance tasks could inadvertently introduce errors into the system that may affect how effectively these subsystems operate.

Conclusion

DLC.Link uses Bitcoin's DLCs to allow developers to integrate native Bitcoin into smart contracts. Swap authorization is implemented via a quorum mechanism that uses third-party independent entities called attestors.

This architecture ensures security through attestor honesty, a mechanism upheld by the quorum mechanism. This approach decentralizes the system and strengthens its security posture by requiring consensus among multiple attestors, thus minimizing risks of collusion or malicious intent.

Unlike traditional bridges that typically rely on a single central entity for trust, DLC.Link offers a safer experience by utilizing external attestors to validate transactions and contracts across different blockchains. Unlike a bridge, the funds are not held by a set of bridge validators where they could be stolen if the bridge was hacked, but rather in a simple multi-sig between the two counter-parties with a set of partially signed outcomes, with no way for funds to be stolen by a third party

The strength of the DLC.Link system's security lies in its adept utilization of secure individual components. By harnessing the inherent security of DLC contracts, the Bitcoin blockchain and quorum-style validation through attestors, the system establishes a sound design from a security point of view.

Changelog

- 2023-08-08 – Initial report.
- 2023-08-09 – Fixing typos.
- 2023-08-17 – Improve service description.