TL;DR

This proposal presents a practical trustless Bitcoin bridge using Nillion's NMC (Nil Message Compute) protocol. The bridge leverages secure encryption, secret sharing, and cross-chain witness validation to enable the secure and decentralized transfer of Bitcoin to other blockchains.

Background

Interoperability between different blockchains is crucial for the growing decentralized ecosystem. Trustless bridges allow secure transfers of assets and information across blockchain networks without relying on a central trusted authority. Nillion's NMC protocol provides a framework for creating such trustless bridges.

Proposal

The proposed trustless Bitcoin bridge consists of the following steps:

1. Initial Encryption

:

- The Bitcoin secret key K

is encrypted using a symmetric encryption scheme $E = (\text{Enc}, \text{Dec})$

with a condition-based ciphertext C

dependent on a predefined condition Φ

on a separate blockchain, such as Ethereum:

$$C = \text{Enc}(K, \Phi)$$

1. The Bitcoin secret key K

is encrypted using a symmetric encryption scheme $E = (\text{Enc}, \text{Dec})$

with a condition-based ciphertext C

dependent on a predefined condition Φ

on a separate blockchain, such as Ethereum:

$$C = \text{Enc}(K, \Phi)$$

1. Generating Particles

:

- A One-Time Mask (OTM) is applied to the ciphertext C

to generate masked particles ${p_i}_{i=1}^n$

:

$$p_i = C \oplus b_i \quad \forall i \in [1, n]$$

where ${b_i}_{i=1}^n$

are random blinding factors.

1. A One-Time Mask (OTM) is applied to the ciphertext C

to generate masked particles ${p_i}_{i=1}^n$

:

$$p_i = C \oplus b_i \quad \forall i \in [1, n]$$

where ${b_i}_{i=1}^n$

are random blinding factors.

1. Blinding Factor Sharing

:

- Linear Secret Sharing (LSS) is used to distribute the blinding factors $\{b_i\}_{i=1}^n$

among a decentralized network of nodes $\{N_i\}_{i=1}^n$

.

- Polynomials $f_i(x)$

of degree t

are constructed for each blinding factor b_i

:

$$f_i(x) = b_i + a_1 x + a_2 x^2 + \cdots + a_t x^t$$

- n

shares $\{s_{i,j}\}_{j=1}^n$

are generated for each blinding factor b_i

by evaluating $f_i(x)$

at distinct points $x_j \in \mathbb{F}_p$

:

$$s_{i,j} = f_i(x_j) \quad \forall j \in [1, n]$$

- The shares are distributed to the corresponding nodes N_j

.

1. Linear Secret Sharing (LSS) is used to distribute the blinding factors $\{b_i\}_{i=1}^n$

among a decentralized network of nodes $\{N_i\}_{i=1}^n$

.

1. Polynomials $f_i(x)$

of degree t

are constructed for each blinding factor b_i

:

$$f_i(x) = b_i + a_1 x + a_2 x^2 + \cdots + a_t x^t$$

1. n

shares $\{s_{i,j}\}_{j=1}^n$

are generated for each blinding factor b_i

by evaluating $f_i(x)$

at distinct points $x_j \in \mathbb{F}_p$

:

$$s_{i,j} = f_i(x_j) \quad \forall j \in [1, n]$$

1. The shares are distributed to the corresponding nodes N_j

.

1. Particle Distribution

:

- The masked particles $\{p_i\}_{i=1}^n$

are distributed across the decentralized network of nodes $\{N_i\}_{i=1}^n$

.

- Each node N_i

holds a single particle p_i

.

1. The masked particles $\{p_i\}_{i=1}^n$

are distributed across the decentralized network of nodes $\{N_i\}_{i=1}^n$

.

1. Each node N_i

holds a single particle p_i

.

1. Witness Condition Validation

:

- Upon fulfillment of the predefined condition Φ

on the Ethereum blockchain, a witness proof π

is generated.

- Nodes validate the witness proof π

to initiate the reconstruction process.

1. Upon fulfillment of the predefined condition Φ

on the Ethereum blockchain, a witness proof π

is generated.

1. Nodes validate the witness proof π

to initiate the reconstruction process.

1. Reconstruction and Decryption

:

- Nodes collaborate to reconstruct the blinding factors $\{b_i\}_{i=1}^n$

using the LSS shares:

$b_i = \sum_{j \in I} s_{i,j} \prod_{k \in I \setminus {j}} \frac{x_k}{x_k - x_j}$

where $I \subseteq [1, n]$

and $|I| = t + 1$

.

- With the reconstructed blinding factors $\{b_i\}_{i=1}^n$

, nodes unmask their particles p_i

to recover the original ciphertext C

:

$$C = p_i \oplus b_i \quad \forall i \in [1, n]$$

- The recovered ciphertext C

is decrypted using Dec

and the condition Φ

to obtain the Bitcoin secret key K

:

$$K = \text{Dec}(C, \Phi)$$

1. Nodes collaborate to reconstruct the blinding factors $\{b_i\}_{i=1}^n$

using the LSS shares:

$$b_i = \sum_{j \in I} s_{i,j} \prod_{k \in I \setminus {j}} \frac{x_k}{x_k - x_j}$$

where $I \subseteq [1, n]$

and $|I| = t + 1$

.

1. With the reconstructed blinding factors $\{b_i\}_{i=1}^n$

, nodes unmask their particles p_i

to recover the original ciphertext C

:

$$C = p_i \oplus b_i \quad \forall i \in [1, n]$$

1. The recovered ciphertext C

is decrypted using Dec

and the condition Φ

to obtain the Bitcoin secret key K

:

$$K = \text{Dec}(C, \Phi)$$

Advantages

The proposed trustless Bitcoin bridge has several advantages:

- Decentralization

: The use of a decentralized network of nodes eliminates the need for a central trusted authority.

- Security

: The encryption and secret sharing techniques ensure the confidentiality and integrity of the Bitcoin secret key.

- Cross-chain interoperability

: The bridge enables the secure transfer of Bitcoin to other blockchains, such as Ethereum, based on predefined conditions.

- Fault tolerance

: The use of Linear Secret Sharing provides fault tolerance, as the secret can be reconstructed even if some nodes are unavailable or malicious.

Applications

The trustless Bitcoin bridge has various applications, including:

- Cross-chain asset transfers

: Enabling the seamless transfer of Bitcoin to other blockchains for use in decentralized applications (DApps) and decentralized finance (DeFi) protocols.

- Atomic swaps

: Facilitating atomic swaps between Bitcoin and other cryptocurrencies without the need for a trusted intermediary.

- Conditional payments

: Allowing for conditional Bitcoin payments based on events or conditions on other blockchains.

Conclusion

The proposed trustless Bitcoin bridge using Nillion's NMC protocol provides a secure, decentralized, and interoperable solution for transferring Bitcoin across different blockchain networks. By leveraging cryptographic techniques such as encryption, secret sharing, and cross-chain witness validation, the bridge ensures the integrity and confidentiality of the transferred assets. This proposal opens up new possibilities for cross-chain asset transfers, atomic swaps, and conditional payments, further enhancing the interoperability and composability of the decentralized ecosystem.

[Nillion Whitepaper]