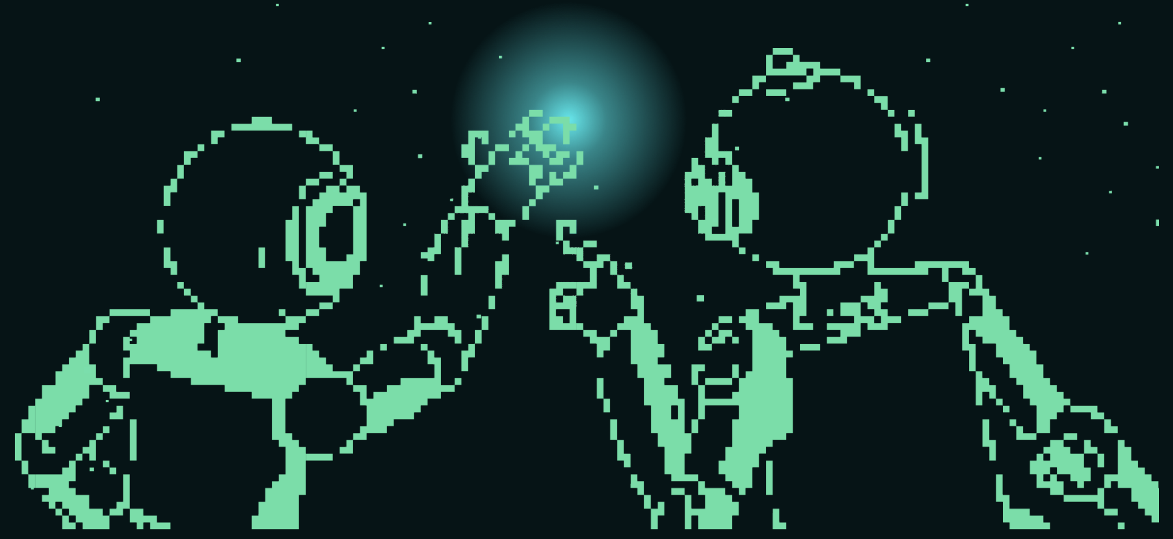
MIND NETWORK

Building a Zero Knowledge Proof-Based BTC Bridge

ABCDE ZK Hacker Camp



Team: ZkBTCBridge

Date: 2023.09.15

Singapore

Agenda

1. Introduction

2.BTC Bridge problem definition

3. Our solution: ZKP-Based BTC Bridge

4. Conclusion with future developments

Introduction

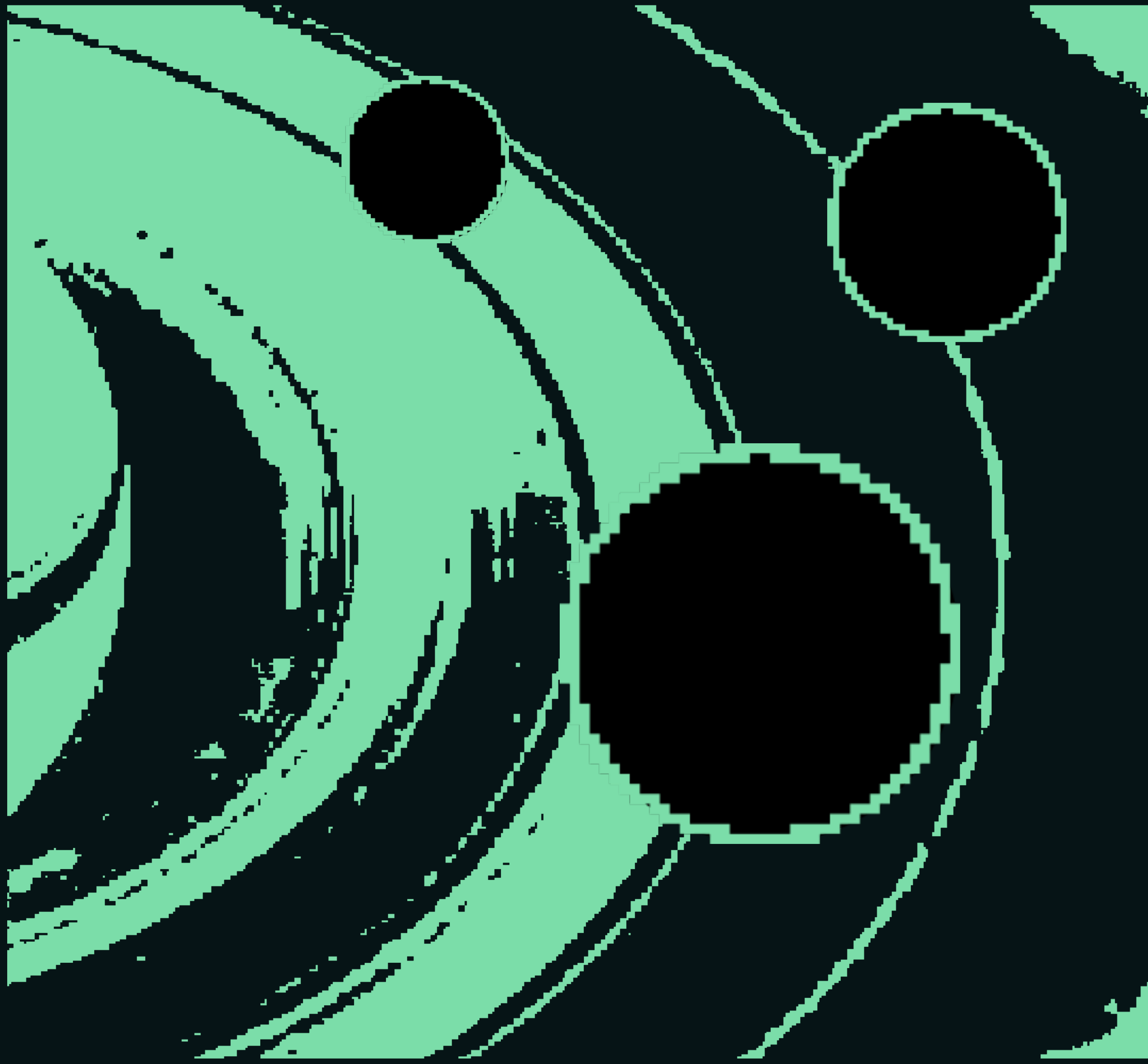
- What is a BTC Bridge

A BTC Bridge, in the context of blockchain and cryptocurrency, is a mechanism or platform that allows users to transfer Bitcoin (BTC) tokens or assets from one blockchain network to another.

These bridges serve as a link or connection between different blockchain ecosystems, enabling users to move BTC between them.

- Why we need a BTC Bridge

It is not easy to transfer a bitcoin to the Ethereum blockchain because the Bitcoin blockchain and the Ethereum blockchain operate independently. A BTC Bridge addresses this interoperability challenge by providing a secure way to transfer BTC tokens from one blockchain to another.



Problem Definition

Design and implement a secure and efficient BTC Bridge that enables the transfer of Bitcoin (BTC) from a Bitcoin blockchain address to an Ethereum blockchain address while preserving the security, integrity, and trust of the assets being transferred.

Interoperability

“ Create a bridge that facilitates the seamless transfer of BTC between the Bitcoin and Ethereum blockchains, allowing users to utilize their BTC holdings on the Ethereum network.

Trustworthiness

“ Establish trust in the bridge by employing transparent and verifiable processes for asset custody, transfer, and verification.

Security and Privacy

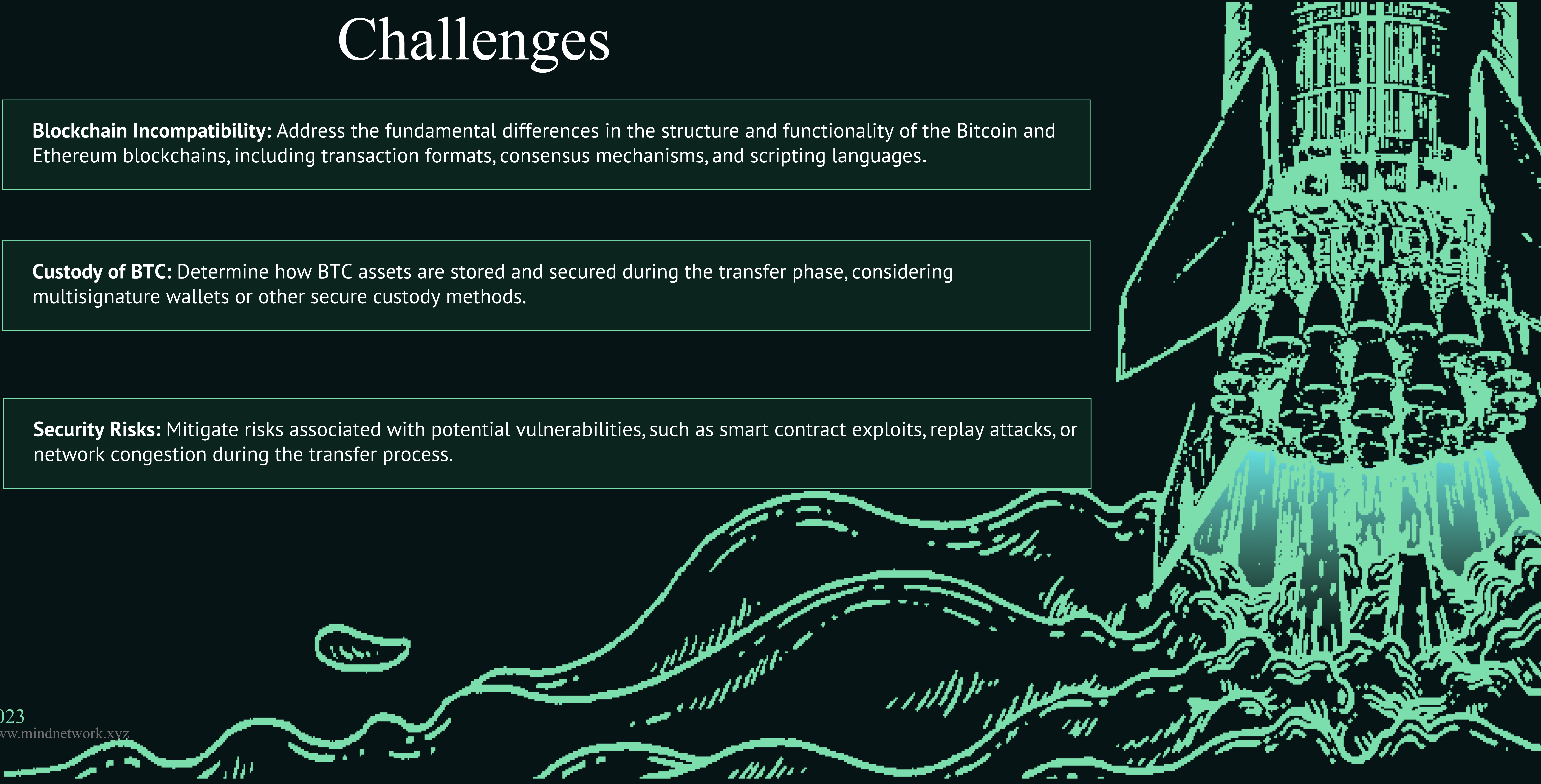
“ Ensure that the bridge design includes robust security measures to protect user assets during the transfer process, minimizing the risk of unauthorized access or theft.

Challenges

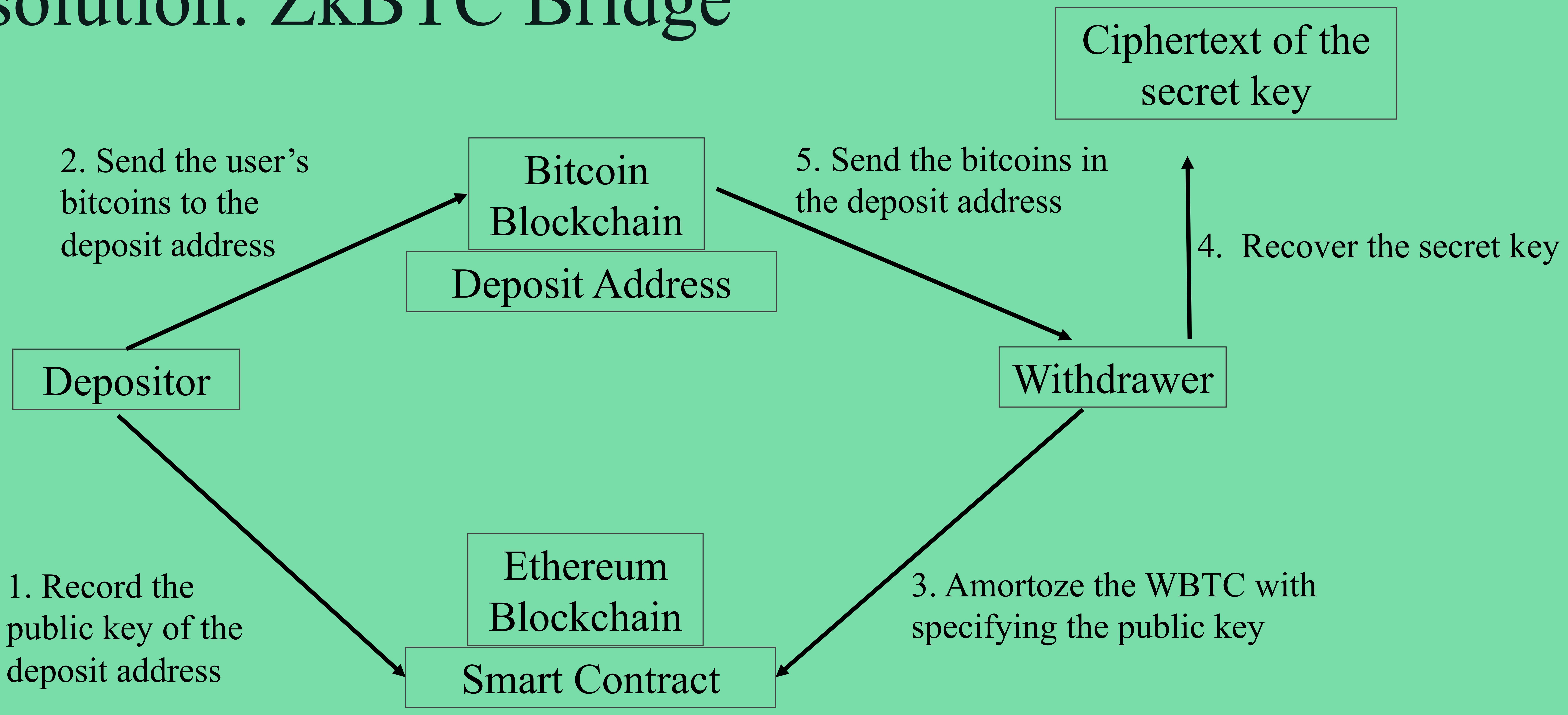
Blockchain Incompatibility: Address the fundamental differences in the structure and functionality of the Bitcoin and Ethereum blockchains, including transaction formats, consensus mechanisms, and scripting languages.

Custody of BTC: Determine how BTC assets are stored and secured during the transfer phase, considering multisignature wallets or other secure custody methods.

Security Risks: Mitigate risks associated with potential vulnerabilities, such as smart contract exploits, replay attacks, or network congestion during the transfer process.



Our solution: ZkBTC Bridge


Ciphertext of the secret key
2. Send the user's bitcoins to the deposit address
Bitcoin Blockchain
Deposit Address
5. Send the bitcoins in the deposit address
4. Recover the secret key
Depositor
Withdrawer
1. Record the public key of the deposit address
Ethereum Blockchain
Smart Contract
3. Amortoze the WBTC with specifying the public key

Deposit Bitcoin - Zero knowledge implementation

We implement functionality of a light client in the Bitcoin network as part of the circuit used by the NIZK proof system. bitcoin deposits can be realized securely by 1 to 6 as follows:

1.The format of each block header is correct (e.g., the nonce of each block header satisfies the PoW constraints).

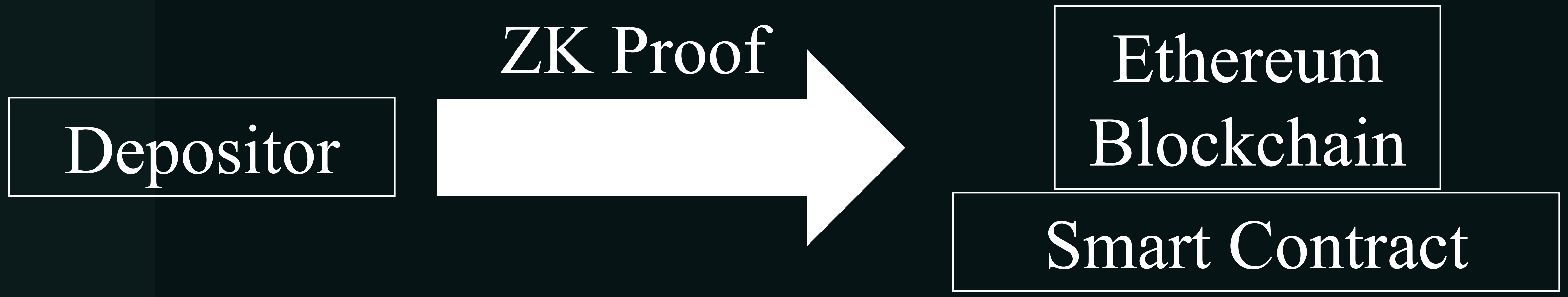
2.Except for the last block header, the block hash of each block header is referenced as the previous block hash in the block header that follows it.

3.The first block header is the one that follows the finalized block header. However, the finalized block header is determined during address generation.

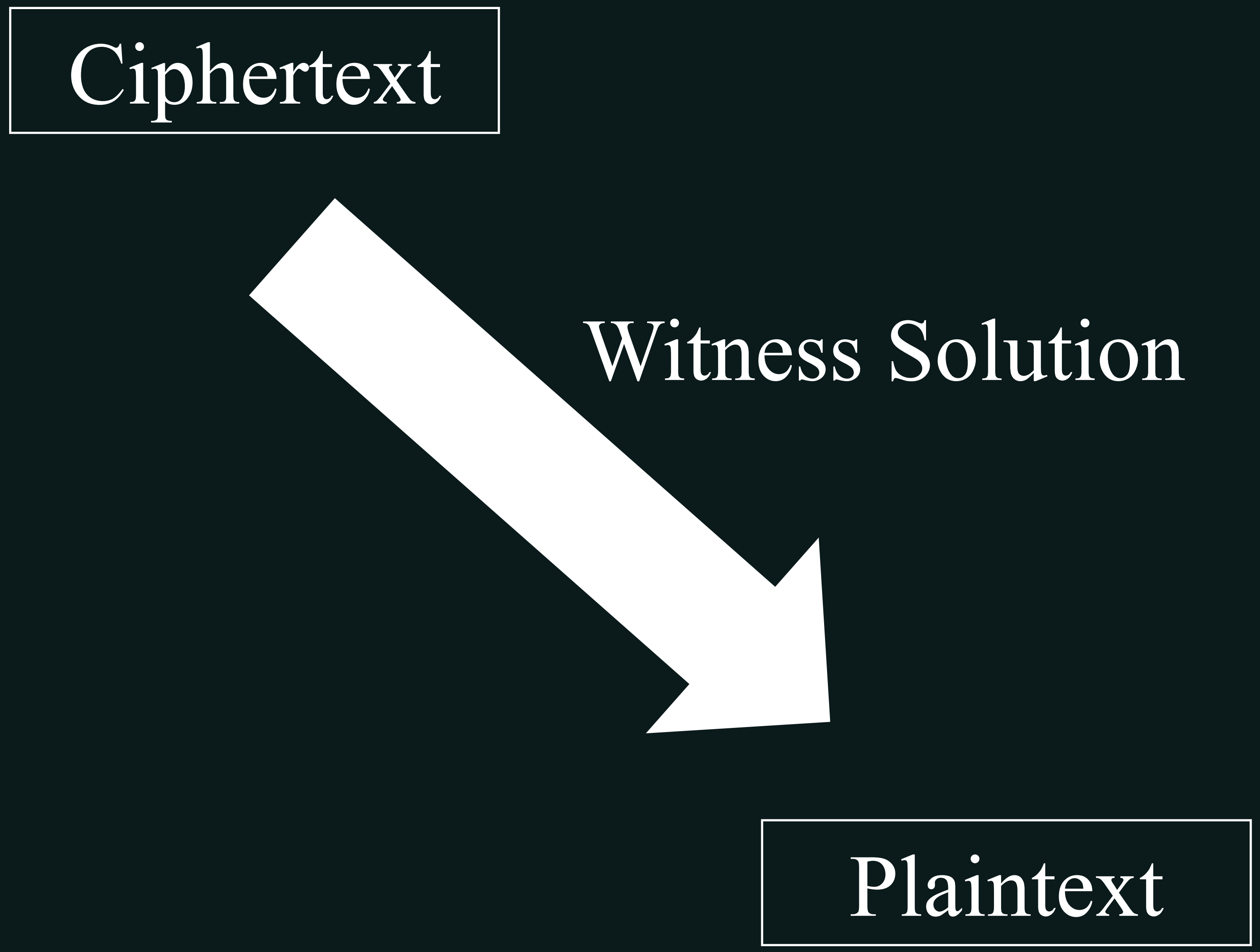
4.The cumulative difficulty value is greater than the given minimum cumulative difficulty value in the last block header.

5.The transaction format is correct, and its hash value is contained in the Merkle Root in the block header at the specified block height.

6.The recipient's address in the transaction is equal to the deposit address, and the transfer amount is equivalent to the value fixed in the system.



Withdraw Bitcoin – Witness encryption implementation



Ciphertext

Witness Solution

Plaintext

- Key generation and witness generation
- Encryption: The encryption process also takes the data, private key and witness information into account, which generates the ciphertext.
- Decryption: To decrypt the data, the recipient needs both the decryption key and the correct witness.If the correct witness is provided along with the decryption key, the decryption algorithm can recover the original data.

Success Criteria:

1. Successful and secure transfer of BTC from a Bitcoin address to an Ethereum address.
2. Minimal downtime and disruptions during the transfer process.
3. Transparent and auditable transaction records and proofs.
4. User feedback and satisfaction with the bridge's functionality and security.
5. Compliance with relevant regulatory guidelines.

Conclusion

We proposed the zkBTCBridge: a WBTC configuration using Zero-knowledge proof and Witness Encryption. This eliminates the need for trusted custodians or individuals to cooperate in guaranteeing the value through overcollateralization.