Blockchain Researcher Intern Assignment

Detecting Cross-Chain Transactions for a Given Address

Objective: Develop a Go-based backend solution that identifies cross-chain transactions associated with a specified address. The system should determine if any transactions from the given address involve cross-chain mechanisms and, if so, identify the target address where
the funds are received.

Tasks:

1. Selection of Blockchain and DEX

Blockchains: Bitcoin, Ethereum
DEX: Uniswap
Blockchain.com | Buy Bitcoin, Ethereum and more with trust API

2. Research and Analysis:

Investigate the mechanisms and protocols used for cross-chain transactions involving the selected blockchain.

Cross-chain Bridge Business Logic[1]

Cross-chain bridges are decentralized applications that serve as channels connecting different blockchain networks, enabling the transfer and exchange of assets and data across different chains. Implementation of cross-chain bridges can be achieved through methods such as atomic swaps, relay chains, sidechains, etc. Typically, a normal and complete cross-chain bridge business workflow will have three phases: source chain, off-chain, and target chain. As shown in Fig. 1, the complete cross-chain flow is demonstrated.

On source Chain: (1) The user initiates a deposit transaction request on the source chain to the router smart contract of the cross-chain bridge. (2) The router contract forwards the request to the corresponding token contract. (3) The token contract locks the asset in the vault and generates a lock event. (4) The Router contract verifies the authenticity of the locking event, and then generates the deposit event.

Off chain: (5) The source chain message is passed down the chain. (6) The off-chain verifies that the source chain information is reliable and then passes the information to the target chain. The off chain verification methods include native verification, local verification and external verification.

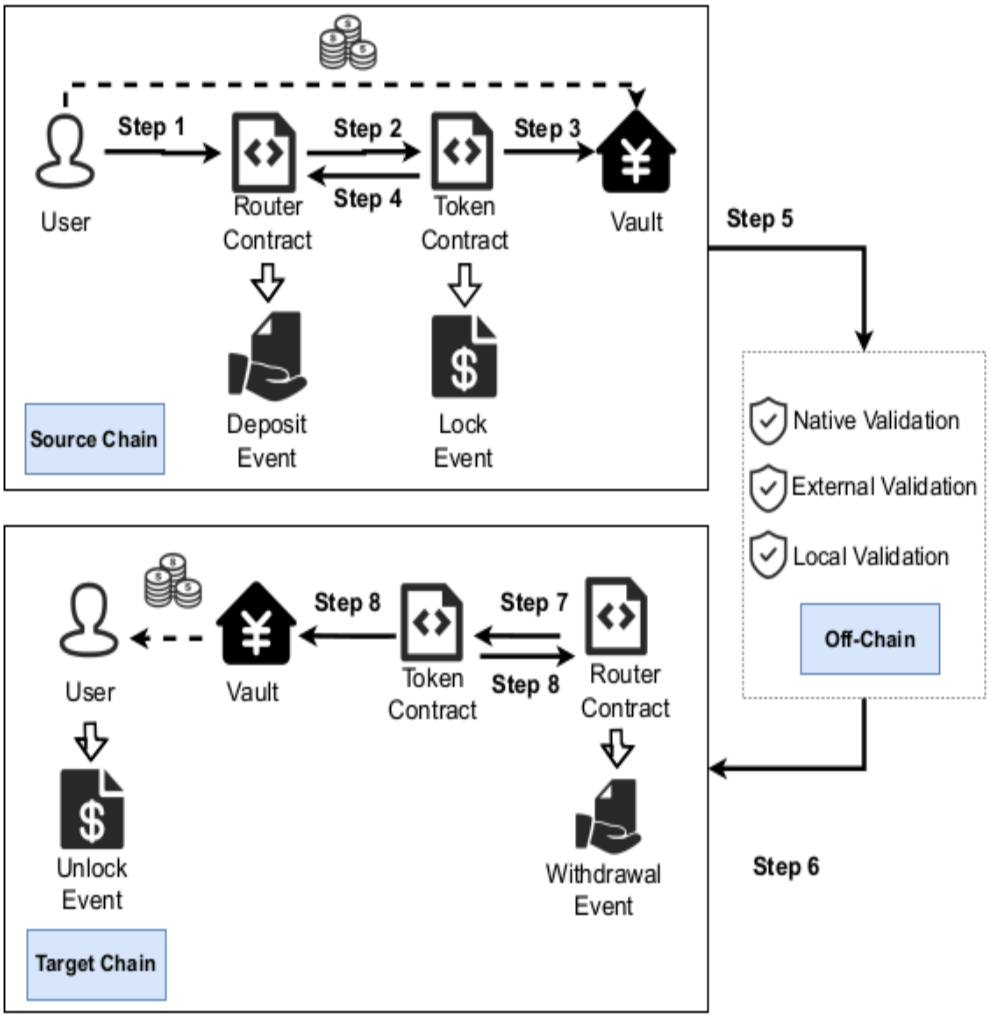


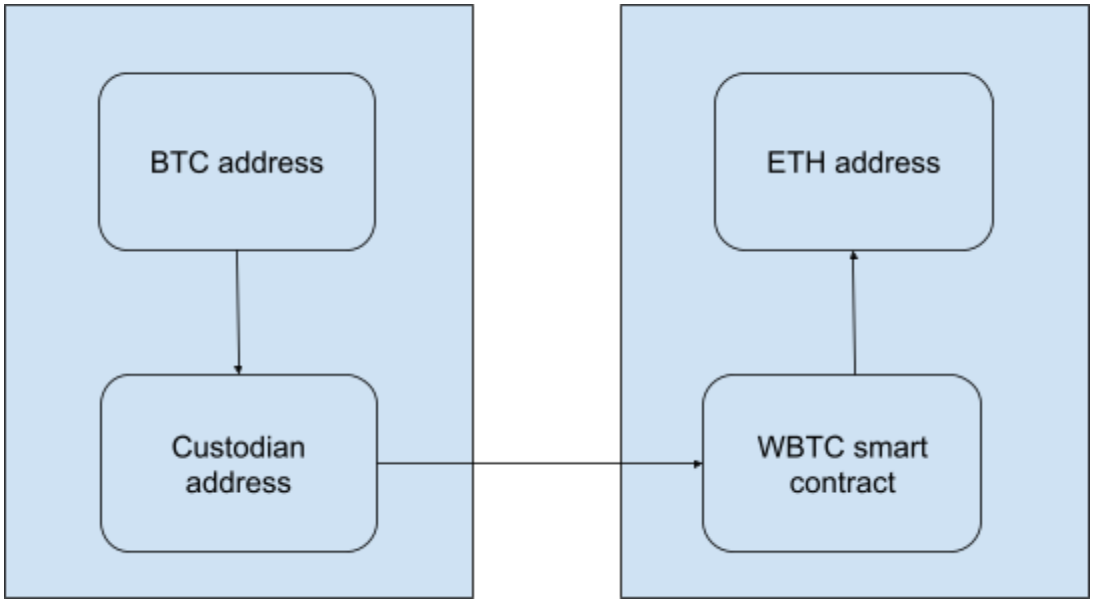
Figure 1: Typical cross-chain bridge procedures.

Source: Safeguarding Blockchain Ecosystem: Understanding and Detecting Attack Transactions on Cross-chain Bridges

On target chain: (7) The router contract forwards the verified request to the token contract. (8) The token contract initiates a withdrawal transaction, which transfers or mints funds from the vault to the user and generates an unlock event. (9) The router contract receives the unlock event and generates the correspond- ing withdrawal event.

The cross-chain transaction process of cross-chain bridges typically involves communication and asset transfer between multiple blockchains, offering users the convenience of cross-chain asset exchange. However, this process also introduces complex security

There is more than one way to perform cross chain transactions. I have focused on cross chain transactions that utilize bridges. Typical methodology in basic terms for BTC to ETH transactions that used these bridge are explained below.



Step 1: Bitcoin Address Sends BTC to a Custodian Wallet

Bitcoin addresses initiate Cross bridge transactions by sending money to Custodian addresses. (e.g., BitGo, which acts as a trusted entity to hold the BTC reserves). These custodian wallets are well known and it will hold bitcoin during cross-chain transactions.

Step2 : Minting Wrapped Bitcoin (WBTC) on Ethereum

After receiving the bitcoin, the Correlated smart contract of Wrapped Tokens on ethereum will mint the WBTC as the same amount of Bitcoin sended to the custodian wallet.

Step 3: Ethereum Address Receives WBTC

Newly minted WBTC will be transferred to the Ethereum account. Now, users can use that WBTC in Ethereum eco-system for trading, staking etc.

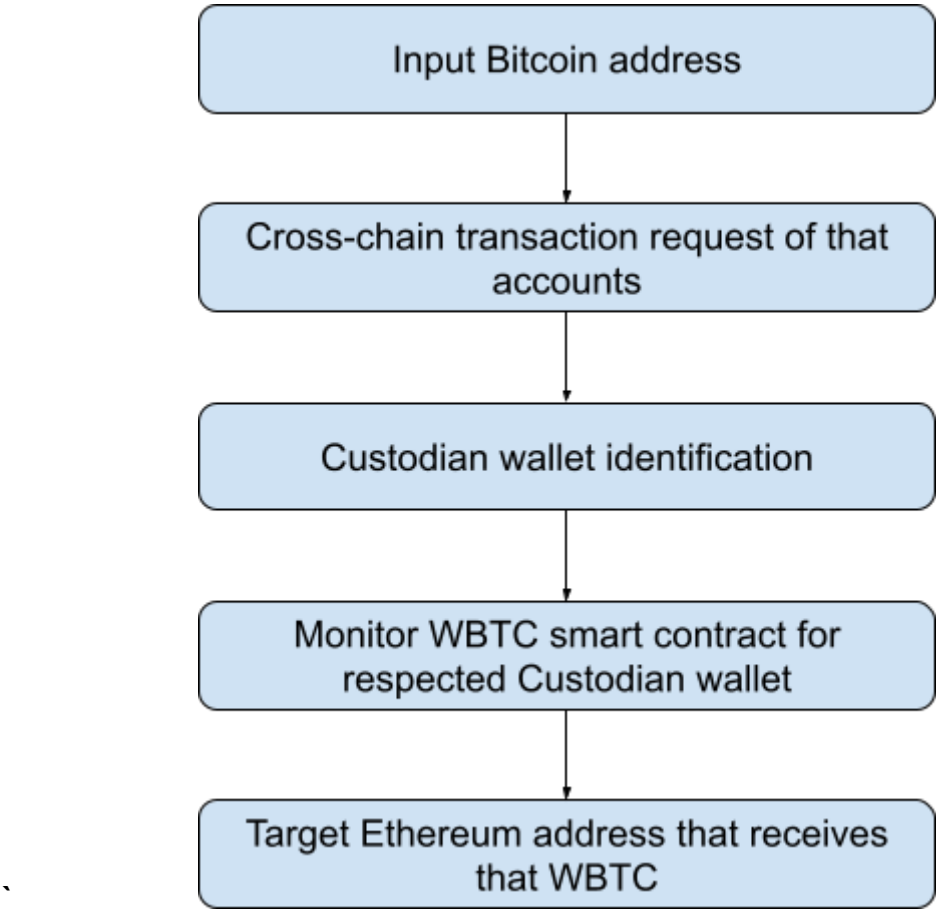
3. Design and Implementation:

Preparation phase: I need a Bitcoin address that contains a cross-chain transaction. What I have searched for is as follows: I have searched for custodian addresses that work as a bridge between bitcoin and ethereum. Here I have find WBTC address: “3FPunzAzeSqYE8ShL1KKCyiJZQAwrsyWPE”

Then I searched for all the transactions related to address “3FPunzAzeSqYE8ShL1KKCyiJZQAwrsyWPE” in bitcoin.com. From there I analyse and

seen from which address founds had came and I found this bitcoin address: “bc1qty432wmpz8sw5dncpqphsh0mnlklurkpcjx7l5r66gdgn0vcvs4sw2phdn”
This is how I got the address that had done the cross-chain transaction. I have used this address for testing purposes during implementation.

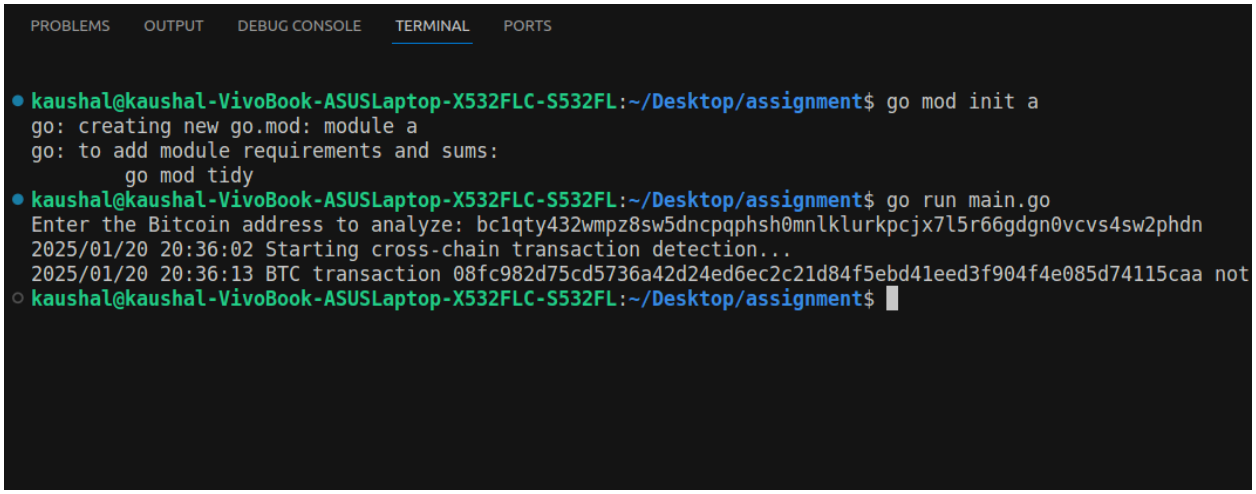
Working Flow of Design

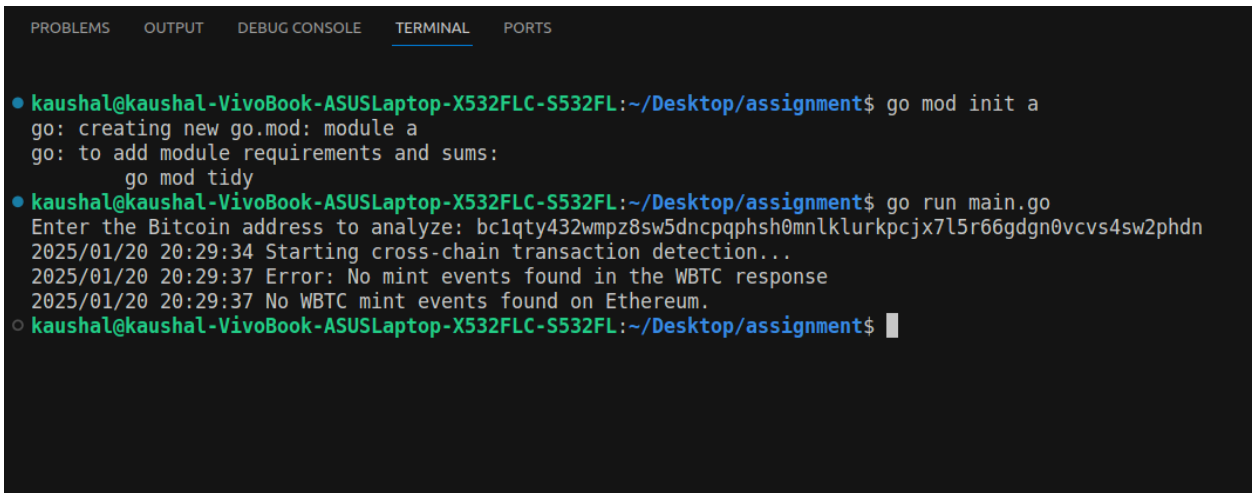


`

- Take Bitcoin address as input from user
- Fetch all transactions related to that address using public APIs and identify cross-chain transactions performed by that address.
- Identify Custodian Wallet associated with cross-chain transactions.
- On the Ethereum blockchain monitor WBTC smart contract for mint events and take note of minted amount and recipient address.
- Correlate the data and you can find the target Ethereum address of the initial Bitcoin sender.

Output





I am unable to find corresponding mint events. But still I am sending my work till i have completed.

References:

- https://www.merklescience.com/decrypting-crypto-bridge-transactions-for-investigations#:~:text=How%20Crypto%20Cross%20Chain%20Transaction,Visualizing%20and%20Investigating%20Transactions
- http://blockchain.com/
- https://www.elliptic.co/blog/tracking-crypto-through-bridges-dexs-and-swaps
- https://arxiv.org/pdf/2410.14493
- https://www.blockchain.com/explorer/addresses/btc/3FPunzAzeSqYE8ShL1KKCyiJZQAwrsyWPE
- https://wbtc.network/dashboard/partners