COMP4901W Homework 7

KIM, Jaehyeok (20550178)

The Hong Kong University of Science and Technology

Exercise 1

Before executing the protocol, let's assume that Alice and Bob have both Bitcoin and Ethereum wallets and know each others' addresses. Also, let each Bitcoin Blockchain and Ethereum Blockchain be $Blockchain_B$ and $Blockchain_E$.

1. Alice first generates a random secret key s and its hash $h(s)$. Then, she creates and deploys a contract C_B (e.g. using *Script*) to $Blockchain_B$ and deposits her 100 BTC to the contract. The contract is with the following functionalities:
   - It has a time limit t_B specifying the deadline for Bob's withdrawal.
   - It sends the deposit to the withdrawer, if:
     - The deadline t_B has not passed yet.
     - The withdrawer address is Bob's Bitcoin address.
     - The hash of the submitted secret matches $h(s)$.
   - If t_B has passed and no valid withdrawal requests existed, the deposit is sent back to Alice's Bitcoin address.

2. Bob then can check C_B on $Blockchain_B$ and verify if the deployer address is Alice. If valid, he can obtain $h(s)$ from the contract and creates and deploys another contract C_E (e.g. using *Solidity*) with his deposit 1333 ETH on $Blockchain_E$ with the following functionalities:
   - It also has a time limit t_E specifying the deadline for Alice's withdrawal and this deadline is sufficiently earlier than t_B so that Alice cannot take both of the assets.
   - It sends the deposit to the withdrawer, if:
     - The deadline t_E has not passed yet.
     - The withdrawer address is Alice's Ethereum address.
     - The hash of the submitted secret matches $h(s)$.
   - If t_E has passed and no valid withdrawal requests existed, the deposit is sent back to Bob's Ethereum address.

3. Once Bob deploys C_E to $Blockchain_E$, Alice can use the secret s before t_E to make the transaction of sending 1333 ETH to her Ethereum address.

4. Once Alice's request is processed or observed from the mempool, Bob can acquire the secret s and submit it to C_B before t_B to make the transaction of transferring 100 BTC to his Bitcoin address.

Explanation:

Since the time limits and the hash checking on each contract successfully protect and restrict any illegal actions by any parties, Alice and Bob can safely exchange their assets on different chains using this protocol. 1333 ETH on C_E can only be withdraw by Alice by providing the valid secret key s. If she does not, it will be safely returned to Bob and Alice will also get back her money safely from C_B. No third-party can withdraw the money from C_E as Alice is the only one who knows the secret key s before she requests for the withdrawal. No third-party can withdraw the money from C_B even with the secret key s since C_B checks whether the requesting address is Bob's or not. Moreover, by Bob setting t_E sufficiently earlier than t_B, Alice cannot try to withdraw both assets at the same time. Therefore, the above protocol following the Hash Time Locked Contract approach allows secure exchange of BTC and ETH that are on the different chains.