COMP4901W Homework 7 Resubmission

Name: Hangyul SON
SID: 20537267

Procedure

1. Bob and Alice both creates a wallet in Bitcoin network and Ethereum network respectively. Both share address to receive the fund on the opposite chain.
2. Bob deploys a smart contract on the Ethereum Blockchain. The smart contract is created under few requirements.
   a. As the contract gets deployed, Bob deposits 1333 ETH and also deploys the hashed version of a 'key' in which is capable of claiming the locked up ETH.
   b. There must be a time bound to retrieve ETH if no key has been submitted until a certain timebound. This is to prevent Bob from locking up ETH given Alice acts maliciously without committing on what was agreed.
   c. The smart contract must send ETH to Alice's address if and only if Alice submits the key, which is yet only available to Bob.
3. Bob send Alice the hash of the key.
4. Alice uses the hash and create a script which sends 100 BTC to Bob on the Bitcoin network. For Bob to claim the BTC, few criteria must be met.
   a. Hashlock: the key submitted by Bob becomes hashed and it must match with the lock within the script.
   b. Timelock: There must be a time bound to retrieve BTC if no key has been submitted until a certain timebound. This is to prevent Alice from Bob acting maliciously without committing on what was agreed. However, the timebound **must** be shorter than the timebound of Bob's smart contract.
   c. If the hasklock and timelock conditions are not met the fund will be returned back to Alice.
5. Bob make use of the key to unlock the contract and receive BTC before the timebound. As Bob submits the key, it becomes available to Alice as well.
6. Alice makes use of the revealed key to claim ETH before the timebound. Given Alice creates a timebound significantly shorter than Bob's timebound, Alice would have sufficient amount of time unlock the ETH.
7. The agreement between Bob and Alice comes to an end.