COMP 4901W - Homework 7

SON Hangyul
SID: 20537267

Assumptions

1. Ethereum blockchain allows smart contracts whereas Bitcoin Blockchain does not.
2. Bitcoin acts as an item (just like in normal good sales) in this protocol and Ether acts as a currency of exchange.
3. Bob and Alice both are born malicious entities. Unless they are disincentivized of their malicious activity they are guaranteed to do it.

Steps

1. Bob and Alice both creates an account on the Bitcoin blockchain and on the Ethereum blockchain. They trade their wallet address.
2. Bob creates a smart contract which is programmed to automatically send ETH to Alice's Ethereum wallet address once Bob receives the BTC from Alice.
3. Alice is aware of the smart contract and can verify the validity of the contract.
4. Bob deposits twice (can be adjusted) the amount of ETH of what Alice must pay Bob in BTC.
    a. EX) Bob deposit 26.66 ETH and Alice must pay 1 BTC. (1BTC = 13.33ETH)
5. As soon as Bob deposits his ETH to the smart contract, a time bound is set. Alice must send her BTC within the time bound.
    a. 1 BTC transferred to Bob's Bitcoin account
6. If Alice refuses to send her BTC to Bob within a certain amount of time, Bob can program his smart contract to transfer back all his ETH deposit.
7. Once Bob receives BTC in his account, Bob directly transfers the same amount in ETH to Alice's Ethereum wallet.
    a. Bob sends Alice 13.33ETH.
8. For Alice to declare and notify the smart contract of her payment in BTC to Bob, she must first deposit the amount of ETH she received from Bob to the contract.
    a. Alice deposits 13.33ETH to the contract
9. The smart contract transfers the exchange amount to Alice. Bob retrieves his deposit back without the exchanged amount. In conclusion, Bob has received BTC and Alice has received the corresponding amount of ETH.
    a. Smart contract hold 39.99ETH.
    b. 26.66ETH is returned to Bob, 13.33ETH is sent to Alice
    c. Bob has 1 BTC, Alice has 13.33 ETH at the end.
10. The transaction can be repeated with larger or smaller amounts of currency until all 1333ETH and 100 BTC is exchanged. However, Bob must always deposit twice or more ETH than the agreed exchange amount to the contract.
    a. Assume Alice and Bob have exactly the same amount of BTC and ETH. Since 1 Satoshi is the smallest unit of currency in Bitcoin, in order to exchange 1 Satoshi with ETH, Bob needs to deposit twice the amount of 1 Satoshi in ETH. If Alice is left with 1 Satoshi, Bob will also be left with amount of ETH corresponding to 1 Satoshi.

The smart contract should handle each of the following cases

1. Bob declares BTC ‘Received’ (Genuine) / Alice declares BTC ‘Sent’ (Genuine)
2. Bob declares BTC not ‘Received’ (False) / Alice declares BTC ‘Sent’ (Genuine)
3. Bob declares BTC not ‘Received’ (Genuine) / Alice declares BTC ‘Sent’ (False)
4. Bob declares BTC not ‘Received’ (Genuine) / Alice declares BTC not ‘Sent’ (Genuine)

- Case 2: Bob can receive BTC from Alice but decide not to send his ETH by declaring he have not received BTC from Alice to the smart contract.
- Case 3: Alice can decide not to send Bob her BTC. But she can declare that she did make the payment and trick the smart contract to pay her ETH.

Therefore, this protocol is focused on disincentivizing case 2 and case 3.

If there is a disagreement between Alice and Bob, the deposited ETH in the smart contract will be locked up.

1. Case 2: Bob has received BTC from Alice. However, Bob decides not to send ETH to Alice’s Ethereum wallet. Following the protocol, Alice should receive ETH from Bob and can notify the contract of the completion of her payment. Now Alice has lost her BTC.
   However, Bob is disincentivized to do such malicious activity because Alice has the potential to buy ETH from elsewhere and declare she disagrees with the smart contract. Alice will lose more money, but Bob will also lose all his deposit. Bob indeed has received BTC, but since there were twice the amount of ETH deposited, Bob will be disincentivized to do the following. In order to further disincentivize Bob from doing such activity is simple, increase the amount of deposit to three times or four times the amount to be exchanged.
2. Case 3: Without sending BTC to Bob, Alice wants to falsely declare her payment and receive ETH from the smart contract. However, Bob will not send Alice the ETH for her to make her declaration. Alice would have to buy ETH herself in order to perform a malicious activity, whether it is to lock up ETH or make the smart contract pay her the ETH. Since the amount of ETH she would receive from the contract is exactly the same as the amount she needs to deposit, she is not incentivized to do the following. Also, Bob will just receive his original deposit back from the contract.