COMP 4901W – Homework 2 Resubmission

Name: SON Hangyul
SID:20537267
Email: hson@connect.ust.hk

Exercise 2

Alice wants to prove to Bob that she has 10 BTC.

1. Design a protocol by which Alice can prove her ownership of 10 BTC to Bob by performing exactly one transaction on the blockchain but keeping her ownership (except for transaction fees).

    1. Alice demands Bob's public key.
    2. Alice creates a new public key identity.
    3. Alice sends her new public key and an encryption of Bob's public key using Alice's new private key to Bob.
    4. Alice sends 10 BTC from original identity to the new public key identity
    5. Bob check real-time that 10 BTC has been transferred to Alice's new account.
    6. Bob can check that Alice is the owner of the new account by decrypting the message with Alice's new public key.

2. Design a protocol by which Alice can prove her ownership of 10 BTC to Bob without performing any transactions. Alice

    Assumption: The public key of Alice and Bob to each other is unknown. If it is each other's public key is known, the account balance and past transactions can be checked.

    1. Alice requires Bob's public key.
    2. Alice sends a message to Bob's public key. Alice's public key as well as an message encrypted with Alice's private key.
    3. If Bob can decrypt the message using the public key Alice has sent, it means that Alice is aware of the private key of the public key. This proves ownership of the public key.
    4. Bob can check the public key's account balance and past transactions and Alice can prove her ownership of 10 BTC.

3. Design a protocol by which Alice can burn the 10 BTC, making sure that they will never be accessible to herself or anyone else, and prove this to Bob.

   Option 1

   1. Alice goes through part 1 and prove her ownership of 10 BTC and her public key.
   2. Alice makes a transaction sending 10 BTC to a public key without an owner. If there is a well known burning address, then Alice can send her coins to the burning address.
   3. The transaction gets processed and is available on the block chain.
   4. Bob can be aware the public key in which the transaction has been made and its amount.

   Option 2

   1. Alice goes through part 1 and prove her ownership of 10 BTC and her public key.
   2. Alice signs a transaction that has a conditional script as an output to 10 BTC to herself. The script can contain information such that no transaction can be further made using the 10 BTC.
   3. The following transaction will be available to the public along with the script. If Bob reads the script and analyze that validity of the script and Alice genuinely would not be able to make use of 10 BTC, then Alice has proven her burnt 10 BTC.

4. In your protocols above, can Bob obtain any information about Alice's past or future transactions, i.e. transactions that were either performed before your protocol or after it? If so, how can Alice defend against this and preserve her privacy?

   Since 1) 2), and 3) all includes an examining a particular public key's balance and past transactions. And the proofs are finalized by matching Alice's identity with a public key.

   However, if Alice continues to use the same public key to make transactions, than Bob will likely know the following future transactions made from the public key.

   The solution is the following.
   Before Alice goes through the procedure, Alice can monetize all 10 BTC. After that Alice can create a new public key identity to purchase 10BTC. The newly created account will not have any association with the past transactions. Alice can then reveal her public key to Bob.

   After Bob is aware of the new public key of Alice and have been assured that Alice does have 10 BTC, Alice can go through the same process of selling 10 BTC and creating the a new account to buy 10BTC in order to prevent Bob from tracking Alice's future transactions.

~~Version 2~~

~~Assumption: Alice and Bob is referred to their public key (Just like in the lectures)~~

1. ~~Alice sends 10 BTC to herself. This requires Alice's signature in order for the transaction to be valid.~~
2. ~~The transaction gets processed and become registered onto the blockchain.~~
3. ~~Bob sees the transaction as part of the blockchain and becomes assured that Alice own 10 BTC.~~

~~Explanation: Bob can be assured because the fact that 10 BTC is registered on the chained means that Alice is not double spending. This means that if the transaction is not yet on the chain, Alice has the possibility of double spending, as if after spending 10BTC on some product and pretending she still owns 10BTC to Bob. However, once the transaction of spending 10 BTC to herself is processed, this means that even if Alice has had made an attempt to double spend, it has failed and Alice is still the owner of 10BTC. Also, a valid transaction requires Alice's signature, and therefore Bob can be assured that no one else pretended in Alice's favor and proved the ownership of 10BTC instead.~~