COMP4901W Homework 2 Resubmission

KIM, Jaehyeok (20550178)

The Hong Kong University of Science and Technology

Exercise 2

1. Protocol of Alice proving ownership of 10 BTC to Bob by performing exactly one transaction without losing the ownership

1. Bob firstly creates a random verification message (e.g. "This is sent only to Alice :)") and privately send it to Alice.
2. Alice creates an encrypted message by signing the message with her private key.
3. Alice then makes a transaction that takes 10 BTC from her address and outputs 10 BTC to the same address (excluding the trasaction fee) and 0 BTC to Bob.
4. At the same time, Alice sends the signed message and her public key to Bob.
5. After the transaction is processed, Bob checks whether the original message is recovered when the signature from Alice is verified with her public key.
6. Bob also hashes the public key and compare it to the address that made the transaction.
7. Accordingly, Bob will be convinced that the address which made the above transaction not only has at least 10 BTC but also is owned by Alice.