COMP4901W Homework 2

KIM, Jaehyeok (20550178)

The Hong Kong University of Science and Technology

Exercise 1

1. **Yes**. For CL, only the central bank can publish the history of all transactions. Although anyone can create accounts and transact, the transactions are only processed and valid when it is added to a ledger. Therefore, the central bank can freeze a specific coin by ignoring or choosing not to include all transactions taking the specific coin as an input.

2. **No**. Since it requires signature of the original owner, ownership of a coin cannot be confiscated or changed.

3. **No**. Since reversing a transaction already on the chain modifies hash values of all succeeding blocks, it will be easily detected by the users who all have the shared ledger.

4. **No**. Since all valid transactions must contain valid signatures of the owners of the inputs, the central bank cannot spend a coin that does not belong to it.

5. **No**. The central bank can possibly identify some users with public key from multiple transactions and other external resources like CCTV videos, for example. However, it is impossible to identify every transaction's payer and payee since the public key can be created as many as possible, and some of users may change their identity for every transaction.

6. **Yes**. As mentioned in 1., the central bank is the entity that publishes new blocks comprises new transactions to the ledger. Therefore, the central bank can set a new regulation that makes transactions to be valid only when full real world identity is provided. This will only allow transactions only if both the payer and the payee are fully identified in the real world.

7. **No**. Since each users can create as many public keys (identities) as possible, there is no way to identify and blacklist a certain individual based on the public keys used in the transactions. The central bank can blacklist a certain address, but not an individual.

8. **Yes**. If those individuals to be whitelisted do not change their public keys (identities) or the central bank keeps a table to addresses of whitelisted people, the central bank can choose to publish only the blocks containing the transactions from them only.

Exercise 2

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

1. Alice and Bob first have a conversation that Alice is going to make a transaction to prove her ownership of 10 BTC.
2. 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.
3. When the transaction is processed, Bob will be convinced that the address with 10 BTC is owned by Alice by verifying the signature on the transaction. Moreover, no one would really do this meaningless and wasteful transaction to Bob. Therefore, Bob will be convinced that the address which made the above transaction is owned by Alice.

2. Protocol of Alice proving ownership of 10 BTC to Bob without performing any transactions

Since Alice only needs to prove that she actually owns an address containing 10 BTC,

1. Alice chooses a message m to sign (e.g. "This is Alice and I own this address :)").
2. Alice creates a signature by signing m using her secret/private key sk that corresponds to the wallet/address containing 10 BTC.
3. Alice then sends the signature and her public key to Bob.
4. Bob then can use Alice's public key pk to verify the signature and he can verify that the public key owns 10 BTC by checking the ledger. By acquiring the recovered message, Bob will also be convinced that Alice contains a private key corresponding to the address with 10 BTC.

3. Protocol of Alice burning 10 BTC

1. Using the proposed protocol in sub-question 2, Alice first shows and proves her address owning 10 BTC to Bob.
2. Alice then makes a transaction of 10 BTC to a **burning address**. Burning address is an address (public key) that no one knows the corresponding private key (e.g. 0x0 for Ethereum). Since no one knows the private key of the burning address, Alice or anyone else will not be able to access the coins. (If there is no well-known burning address, Alice and Bob can collaboratively create a random address. For example, they can choose each half of the address randomly and none of them will be able to find the corresponding private key given the public key.)
3. Since the burning address is generally known to the public, Bob will be able to convinced that Alice actually burnt 10 BTC by checking the transaction that she sent 10 BTC to the burning address from the ledger.

4. Can Bob obtain any information about Alice's past or future transactions?

The answer is Yes. Since Alice is sharing her public key to Bob, Bob can simply look for her public key in the transactions not only done in the past but also to be processed in the future from the ledger. Nevertheless, it can be easily defended by Alice to preserve her privacy by taking a bit more actions before and after the protocols. Alice can simply create a new address specifically created to use in the protocol. In detail, Alice can simply create a new address before she runs the above protocols. She then transacts the required amount of coins to that address and use this address for the protocol. After the protocol is finished, Alice then can transact back the coins to another newly created address and freely use them. By doing so, the address used for the protocol by Alice is only used for this protocol. Thus, there would be only 1 transaction each before and after the protocol that are disclosed to Bob. Bob can suspect that the sender and receiver addresses for those transactions are one of her other accounts, but there is no way to prove it. Accordingly, Alice can better preserve her privacy than before.