Assignment 1 - Understanding Cryptocurrenies

Max Liu

January 16, 2019

1. Data Structures

1.1

UTXO is necessary to keep track of how many coins a user has and to ensure that a user cannot double spend coins (verifying the UTXO is present in the UTXO pool), spend more coins than they have, or artificially add more coins into their account (the validity of the coin can be verified by the blockchain).

1.2

If multiple nodes do not effectively synchronize their UTXO pools it would be possible for malicious nodes to double spend coins. Nodes that have not heard the initial transaction would believe that the UTXO is valid.

1.3

For the GoodCoin, a valid transaction must provide an input of UTXOs in the proper format that can be found in the UTXO pool (and therefore not used), an output of coins that is equal to the total amount of coins input, and finally the transaction time cannot have occurred in the future. A transaction can also be valid if a node mines a new block by solving a POW and adding the pending transactions to the blockchain, this would result in a reward to the node.

2. Consensus

2.1

The GoodCoin uses the longest blockchain when it tries to resolve conflicts in blockchain versions. This has the benefit of solving forks when they appear as eventually one blockchain will outpace the other chain, ensuring that the blockchain with the most work done is the winner. Furthermore, this makes it difficult for malicious nodes to tamper with existing blocks. However, this can also result in lost blocks if a shorter blockchain contains blocks that are not in the longer blockchain (similarly, an adversary that is able to grow a very long blockchain can cause all nodes to switch to the malicious blockchain).

2.2

The node needs to solve for a proof such that the hash of the last proof, the proof, and the last hash results in a hash with 4 leading zeros.

2.3

In general, a proof of work is used in a blockchain to prevent malicious nodes from building a blockchain that is consistently longer than the consensus blockchain and having the network accept the malicious blockchain. Once the consensus blockchain is ahead of the malicious blockchain it becomes exponentially difficult for the malicious nodes to catch up so they have to give up and move to the consensus blockchain.