Project Overview

Shoma Mori

October 29, 2019

1 Nodes

There are two types of nodes in the system, namely, server and client. Servers are basically validators, who verify transactions. Clients are nodes who issue transactions. Servers behave independently and so do clients, which means the system is asynchronous.

2 Transactions

The following is the flow that describes how a transaction from client c_1 to c_2 is approved by the system without a consensus.

1. c_1 creates a transaction that indicates a payment from c_1 to c_2 using UTXO linked to c_1.
2. c_1 sends the transaction to all servers.
3. The servers verify the transaction by checking whether there is the input as UTXO in their local storage.
4. If there is, the servers send c_1 the transaction with their own signatures which were generated from their private keys, then, discard the input and add the output as UTXO (which is linked to c_2) in their local storage.
5. When c_1 receives valid signatures from more than two-thirds of all nodes, the transaction is regarded to be approved.
6. After the approval, c_1 sends the transaction to c_2 with its signatures.
7. c_2 verifies the signatures using the corresponding public keys and complete the payment.

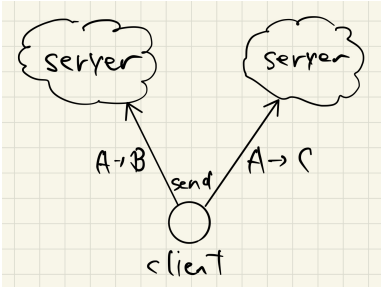

Figure 1: Double-spending

3 Double-spending

Consider the situation that one client sends transactions that imply double-spending before none of them are not approved (Fig. 1). If a server receives more than one transaction of them, it can obviously detect double-spending. If a server receives only one of them (meaning that the byzantine client tried so), the server may sign that transaction. Recall that if the system can assume that the number of byzantine nodes is f and may have more than $3f$ nodes in total, it is proved that the transaction is approved by the system when the transaction gets signatures from 2/3 of all nodes. Now, since the clients cannot send more than one transaction to 2/3 of all nodes without overlapping, more than one transaction cannot be approved. In that case, only one of them would be approved in the best case, and no transactions are approved in the worst case.