Double Spending Fork Attack in Blockchain

I-Ping Tu

Academia Sinica

Abstract

Blockchain has served as a trust ledger structured as a chain of blocks without an administration center through a set of rules coded in a peer-to-peer network system. Each block contains a batch of verified transactions and a cryptographic hash of the prior block that links the blocks. The mining winner who surpasses others on solving a hash function can authorize a block and broadcast it to each node to be updated. A fork in blockchain is a description of two or more chain branches generated from a block and this may happen when two or more miners solve the hash function around the same time. A blockchain fork opens the door to double spending attacks. Satoshi Nakamoto warned a 51% attack in the first bitcoin paper 'Bitcoin: a peer-to-peer electronic cash system' (2008) that if an attacker controls over half of the total hash mining power, that attacker has the capability to execute a double spending fork attack in that blockchain. Historical record never shows a fork exceeding 6 blocks in the bitcoin bolckchain and this explains why bitcoin transactions has a rule of 6-block-confirmation. However, a 51% double spending fork attack did happen on May 18, 2018 in the BTG blockchain and this caused the cryptocurrency exchanges a loss of 1.75 million US dollars. In this talk, we will discuss the double spending problem of blockchains and propose a possible solution. This is a joint work with Jen Chen, Yu-Jing Lin, Huei-Lun Siao, and Shih-Wei Liao.