Lecture 2 – Bitcoin overview summary – Tien Dat Le

Bitcoin is considered as one of the first ledger-based cryptocurrency that can achieved decentralized by successfully solving a class of distributed consensus problem specifically for a currency system. There are 3 main mechanisms that assist Bitcoin to work correctly without relying on a centralized party: Proof-of-work to defense against Sybil attack, a economically driven incentive to force all the nodes to act honestly and a trivial to verify ledger so that all the nodes in the network can verify if the ledger is legitimate or not.

As Bitcoin network is a peer-to-peer network that is not required node's identity, it is trivial for a malicious adversary to create and manipulate as many as participants as he wants. In order to defense to what so-called this Sybil attack, there must be a resource to be chosen for representatives of participants for which it is expensive to have. For proof-of-work in bitcoin, it is the computing resources that a node must have in order to solve the hash puzzle problem in order to propose a new block which will be attached to the ledger. This resulted in an important player in Bitcoin network called miners, which are the ones contribute to the secure of the network.

In addition to defense from Sybil attack, by introducing to the traditional models for consensus the new idea of incentives, Bitcoin succeeded to force the nodes to act honestly. There are 2 main incentives that the honest nodes will receive: a block reward and a transaction fee if they propose a new legitimate block.

There are currently many attacks that can occur in a bitcoin network:

1. Denial of service attack: if the nodes (normally the miners) can propose new block refuse to take transaction from some users, it can prevent them from spending the coin. However, due to the assumption that there will be enough honest nodes, this is not likely a serious attack.
2. Double-spend attack: If Alice spend a bitcoin to Bob and the transaction is attach to a block, and later she tries to create another block with another transaction to send this coin to another address. One of the block will end up discards from the consensus branch, and it is the first one, then Alice is successful do a double-spend attack to Bob. To prevents this, normally Bob have to wait for a couple confirmation (normally 6) to the blocks before classify that he received the coin.
3. 51-percent attack: It is not easy for Alice to do double-spend attack if she does not have more than 51-percent of computing resource, as after 6 confirmations the probability of the block to become orphan is significantly low. However, if Alice have more than 51-percent of computing resource, she can always create a private chain with more confirmation than the main chain, do the double-spend and then broadcast the private chains so that it become the main chain and make that a severe problem of bitcoin networks.

The ledger of Bitcoin is consisted of a linked list of blocks cling with a hash pointer to the previous block right before it hence made Bitcoin ledger tampered resistant. Bitcoin block normally have a list of inputs and outputs. Input will contain the coin from previous output which is not spent and a script signature to prove that the user has a legitimate right to spend the coin in that output. Bitcoin supports a script language so that there are many use

cases can be applied to spent the coins in an output such as: multi-signature spend coins, smart contract, etc.

Just as any distributed software systems, one of the challenge in Bitcoin network is software update. For any changing in the protocol, they will either have to do a soft-fork or a hard-fork which might result in very severe consequences when buggy code happened.