Name: Arnab Rahman Chowdhury **Date: 31 May 2019**

Topic title: Discuss how significant is the number of confirmations in Bitcoin to be 6 or more.

Blockchain Confirmation:

When a user A sends some cryptocoins to user B, the information first broadcasts from the sender's wallet to the cryptocoin network. Network verifies the sender has more coins in his/her wallet than he sends, and the coins are not spent before. After validating the information, miners will include the transaction in a new block along with other transactions in the blockchain. This process is called transaction confirmation.

In other words, blockchain confirmation means how many blocks are added to the blockchain ledger after a block with valid transactions is added to the blockchain ledger. When any transaction is broadcast to the blockchain network for the first time, it is marked as zero confirmation. If any miner receives the transaction from the unconfirmed pool of transaction, solve the "proof-of-work" puzzle, add the transaction to the mined block and add the block to the main blockchain ledger then the transaction will be marked as one confirmation. So as the rest of the transactions on that block.

Why blockchain confirmation is need?

Blockchain confirmation is needed to reduce the double spending attack and to confirm valid transaction. If the attacker has more hash power, then the chance of double sending increases more. According to the survey, even 60 confirmations have <1% odds of succeeding against an entity with 40% hash power. This website (https://people.xiph.org/~greg/attack_success.html) can calculate the probability of successful double send by providing a hashrate proportion and number of confirmations. If the hashrate is 40% and the number of confirmations is 6 then the probability of double sending reaches at 50%.

There are different types of double spending attack in bitcoin network:

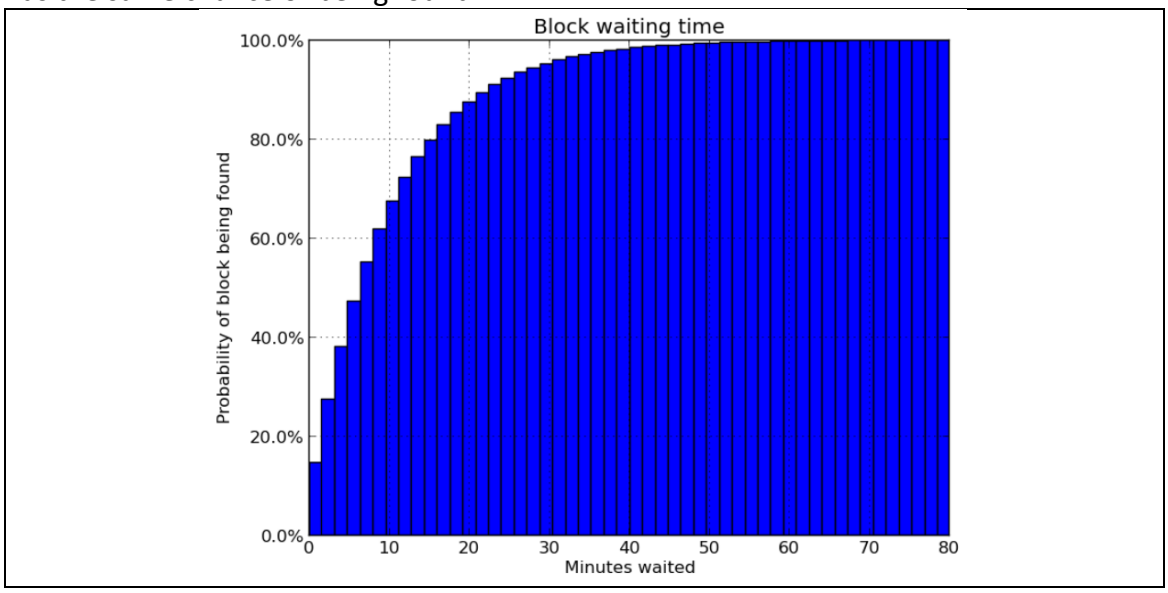
1. Regular double spending attack
2. Finney Attack
3. Race Attack
4. 51% attack

How many confirmations are needed to secure transaction from attack?

Typically, in blockchain network, around 6 confirmations are enough for a secure transaction. Freshly minted bitcoins can only be used after 100 confirmations, to prevent coins from orphan blocks being spent. Suppose, an adversary wants to remove block N from the blockchain ledger. That means attacker needs to fix the block N+1 to point to block N-1. But if there are more blocks after block N then attacker needs to fix all the blocks as each block holds the hash of its previous block. An entity capable of doing this is (thought to be) unlikely.

According to the paper of Meni Rosenfeld,
“If the attacker’s hashrate is 10% of the total network hashrate (0.1 on the horizontal axis), 2 confirmations are required to keep the success rate below 10%, 4 confirmations are needed to have it less than 1%, and 6 confirmations are necessary to decrease the probability of success below 0.1%.”

Bitcoin network takes 10 minutes to add one block in the blockchain but not every block interval is exactly 10 minutes. It follows a statistical process known as a poisson process, where random events happen with the same probability in each time interval. Another way of expressing this is that the mining process has no memory, at every second a block has the same chance of being found.



The number of confirmations depend on the service provider and the amount of coins transfer.

- One confirmation (1) is enough for small Bitcoin payments less than $1,000.
- Three confirmations (3) are enough for payments $1,000 - $10,000. Most exchanges require 3 confirmations for deposits.
- Six confirmations (6) are enough for large payments between $10,000 - $1,000,000. Six is standard for most transactions to be considered secure.
- Sixty confirmations (60) are suggested for large payments greater than $1,000,000.

With more confirmation, the likelihood of a transaction remaining in the public blockchain forever is higher than conflicting transaction if there was one. At 6 confirmations, it is perhaps one in a billion that a transaction won't be permanent.

References:

1. 3 Things to Know about Bitcoin Confirmations (2019 Updated). (2019). Buybitcoinworldwide.com. Retrieved 30 May 2019, from https://www.buybitcoinworldwide.com/confirmations/
2. Bitcoin transaction confirmation. All about cryptocurrency - BitcoinWiki. (2019). En.bitcoinwiki.org. Retrieved 30 May 2019, from https://en.bitcoinwiki.org/wiki/Transaction_confirmation
3. Confirmation - Bitcoin Wiki. (2019). En.bitcoin.it. Retrieved 30 May 2019, from https://en.bitcoin.it/wiki/Confirmation
4. (2019). Bitcoil.co.il. Retrieved 30 May 2019, from https://bitcoil.co.il/Doublespend.pdf