What is 51% attack? How does 51% attack work?

The 51% attack refers to a potential attack on the integrity of the blockchain system, in which a single malicious actor or organization tries to control more than half of the network's total hash power, .

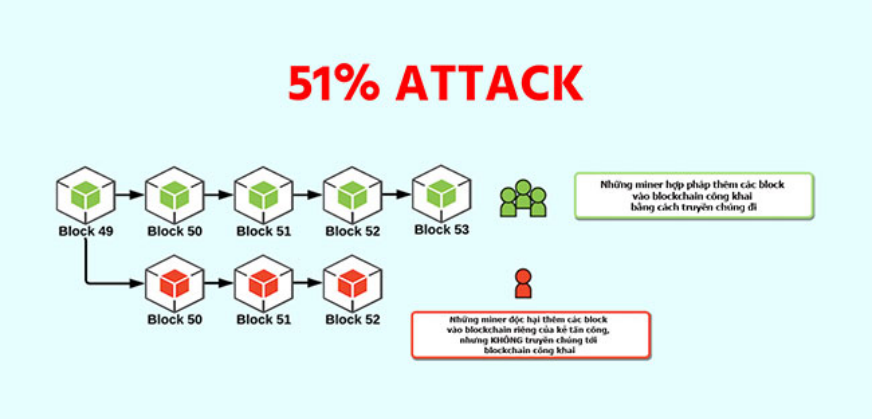
What is 51% attack?

51% Attack refers to a potential attack on the integrity of a blockchain system, in which a single malicious actor or organization seeks to control more than half of the total strength. strong hash of the network, potentially causing network disruption.

How does 51% attack work?

If a bad user or a group of bad users act together, controlling more than 50% of the network's total hash rate in a blockchain, they can override the network's consensus mechanism and take action. micro-toxic.

An attacker will have enough mining power to intentionally modify the order of transactions, preventing some or all of the transactions from being confirmed (also known as transaction denial of service - denial of service.). He can also prevent some or all of the other miners (nodes participating in the blockchain system) from exploiting, resulting in what is called mining monopoly.



For example, if a bad guy takes 51% of the Bitcoin network's hash power, he can perform an OTC transaction offline by sending some Bitcoins to a crypto wallet in exchange for USD. Therefore, as soon as the transaction is confirmed by the network nodes, the buyer (the cryptocurrency trading bot) will innocently hand over USD to the scammer.

The malicious actor can then return to the blockchain before the BTC transfer is confirmed and mine an alternative chain in which the BTC transfer is not included. Much of the network's power will ensure that this is forced to be accepted by the rest of the network as a valid transaction.

How to prevent 51% attack?

On the other hand, a 51% attack does not allow the malicious agent to prevent transactions from being transmitted nor to reverse transactions from other users. Changing block rewards, creating coins from the sky, or stealing coins that don't belong to the attacker are also very unlikely.

The more a transaction is confirmed, the harder it will be to break, as the number of new blocks that are mined to bring the network to its present level becomes greater and more intense. This is why Bitcoin transactions often require a threshold x number of confirmations before making a payment.

A 51% attack on the Bitcoin blockchain is highly unlikely because of the size of the network. As the network grows, the likelihood of a person or entity having enough computational power to overwhelm all the other

participants becomes increasingly unlikely.

Therefore, 51% attacks are very unlikely on major networks, especially on the Bitcoin blockchain, considered the most secure cryptocurrency network. While many major blockchains have not been hacked of this type, the majority have been found on other smaller chains. For example, the Bitcoin Gold altcoin - which is a fork from the main Bitcoin chain - was hit by a 51% attack in May 2018, resulting in the theft of $ 18 million worth of BTG at the time.