What is '51% attack'? Can Bitcoin completely collapse by a 51% attack?

51% attack makes new transactions unable to confirm network congestion, even if an attacker controls the network completely, it can cause the transaction to be reversed.

Over the weekend, hackers made a '51 attack' into Bitcoin Gold cryptocurrency, a cryptographic currency that hardened (branching) from Bitcoin stealing $ 17.5 million. Earlier, the blockchain network of cryptocurrency Verge was also stolen by hackers by more than $ 1.7 million by a "51% attack."

So what is '51% attack'? And does it threaten to cause Bitcoin to collapse?

'51% offensive' is known as a Blockchain system attack controlled by a group of miners more than 50% of the hashrate (a measure of the computing power of the device used to exploit the coins virtual) network implementation. 51% attack makes new transactions unable to confirm network congestion, even if an attacker controls the network completely, it can cause the transaction to be reversed.

For example, I used 100 Bitcoin to buy a Lamborghini supercar. After transferring this money to the car company's wallet, a few days later the Lamborghini was delivered.

By making a 51% attack on Bitcoin's blockchain, I can reverse the transaction. If successful, 100 Bitcoin is still in my wallet while the car is in my possession. I can still use this 100 Bitcoin for other things.

Blockchain = decentralized

The blockchain network is decentralized. Each blockchain network manages a data storage ledger, usually transactional data that is contributed, validated and managed by many computer systems that participate in decoding in the blockchain network around the world. . So the data on the blockchain does not need to be managed by a third party because it is public, transparent, and cannot be modified by any individual. However, it may still exist vulnerabilities and be exploited.

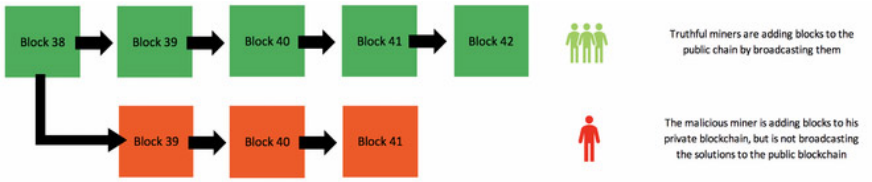
When I transfer 100 Bitcoin to the car company's wallet, the transaction is encrypted and transferred to a place called 'unconfirmed transactions'. These unconfirmed transactions will be chosen by miners to form a block and add to the blockchain network. Miners must solve an extremely complex problem that can be done and this is why Bitcoin excavators require powerful processing and computing hardware.

Miners must compete with each other. The quickest problem solver will be paired with their blockchain. In addition, transactions in this block will be made public and need more than 50% validation by other miners to be shown on the blockchain and transactions recorded in the ledger. Meanwhile, the 100 Bitcoin transfer transaction to buy a new Lamborghini is officially completed.

Miners can only confirm transactions and block blocks into a blockchain and cannot create a transaction themselves, because they do not have the encryption signature of the Bitcoin storage account. Only I have the signature to encrypt my 100 Bitcoin hosting account, so it is impossible to steal my 100 Bitcoin.

The 51% attack will help me duplicate my 100 Bitcoin

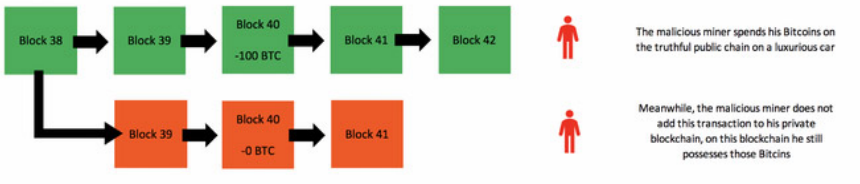
We already know, in order to block our blockchain network, miners must solve the problem quickly. And this Block will be public and requires other miners to confirm with a rate of over 50%.



Blockchain forged orange, unpublished and real Blockchain in blue.

In fact, a miner may not publicize his or her block, and may create a blockchain that is not declared. At that time, I would have two blockchain, a real blockchain confirmed by the majority of miners (in blue) and a fake blockchain not declared (orange).

The purchase of a Lamborghini car with 100 Bitcoin is declared and verified on the true blue blockchain. Miners confirm this transaction and I am deducted 100 Bitcoin in my wallet.



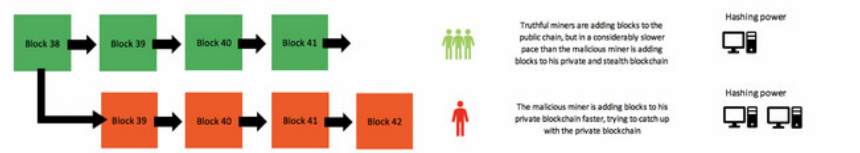
At the real blockchain, the transaction has been confirmed and deducted 100 Bitcoin from the wallet.At the fake blockchain, this transaction does not exist.

But on the orange blockchain, I did not make this transaction and of course I am not deducted 100 Bitcoin in the wallet. Miners are not aware of the existence of this Blockchain because it is not public.

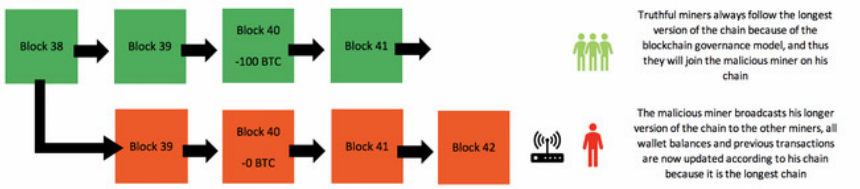
Looking at the image above, we can see the difference in block 40, blue Blockchain has been deducted 100 Bitcoin and the orange Blockchain is not deducted from any Bitcoin. I will copy the next blocks of the blue blockchain (blocks number 41, 42 etc.) to pair and perform the validation itself on the orange blockchain.

Blockchain operates under a democratic governance model, always validating the longest blocks of blocks. Blockchain has the fastest new block speed because it has the participation of many excavators around the world. Here's how to determine which blockchain version is real.

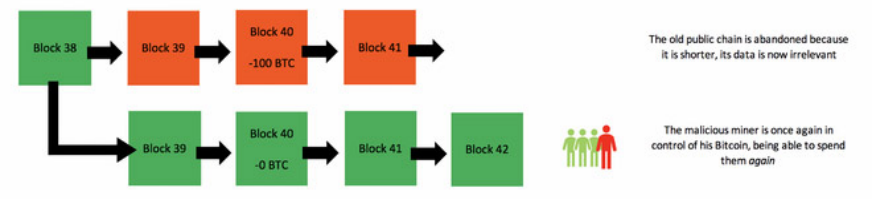
When the race started, I could fool other miners to turn my fake blockchain into a true blockchain if I could add blocks to fake blockchain chains faster than the real blockchain. When there were longer blockchain chains, I publicized my orange blockchain to all other miners.



I can make my fake blockchain have faster validation speed.
Meanwhile, other miners will discover that my fake blockchain is longer than the version they're working on so they will have to switch to the new blockchain.



Blockchain fake turned into a real blockchain.
I have been reversing the transaction successfully, and at the fake blockchain chain, block number 40 that does not carry out Bitcoin transfers and 100 Bitcoin remains in my wallet and the car company's wallet does not of course receive 100 My Bitcoin.



A 51% successful attack.
Why is a 51% attack only in theory? And why did it appear?

Previously, pre-coding experts believed that the 51% attack was only in theory because in order to implement it, hackers must have the power to calculate by 51% the power of all excavators in a network. blockchain grid. And this is impossible.

Specialists believe that a 51% attack will never happen to the world's largest crypto currency, Bitcoin. Because, even the most powerful computers in the world today cannot compete directly with the Bitcoin blockchain's total computing capacity.

To make a 51% attack on Bitcoin blockchain network needs huge computing power.

If someone is able to acquire 51% of the power of a large blockchain network like Bitcoin, they will need to have huge factories, huge amounts of electricity. And this will be very easily discovered by managers.

Yet the 51% attack only existed in theory. In April 2018, there was a 51% attack on Verge. But the reason is that this blockchain network has a flaw that allows hackers not to need actual computing power equal to 51% of the entire network but still be able to create new blocks with lightning speed.

To attack small blockchain requires less computing power than attacking Bitcoin, so a small blockchain of some altcoin may be 51% attacked but with Bitcoin never .

See more:

1. Bitcoin digging around the world consumes electricity in a country
2. The world only has 20% Bitcoin to 'dig'
3. TON - is the crypto currency expected to be the largest ICO in history to be superior to Bitcoin or Ethereum?