51% Attacks explained:

Just mentioning them makes crypto traders freakout, and with good reason. A successful 51% attack against a cryptocurrency would, at best, take a big chunk out of that cryptocurrency's price. And, at worst, could destroy the cryptocurrency altogether.

Put simply, a 51% attack could occur when a malicious actor (or group of actors) controls more than half the mining or hashing power on a blockchain. A 51% attack, also known as a "double-spend attack", allows the attacker to rewrite history on a blockchain. In practical terms, it means the attacker can spend that particular cryptocurrency twice.

As an attacker, one would buy something with bitcoin, then initiate a 51% attack to create a new version of the blockchain – one that doesn't include my transaction. Sounds pretty scary when you put it like that. That said, it is rather difficult to actually pull off a 51% attack on an established network. Bitcoin has never been hit by a 51% attack. Most large cryptocurrencies are safe, software bugs notwithstanding. Some smaller protocols have been attacked. If you can pull one off, you only become a time traveler. You do not have the ability to break the rules of the network, steal cryptocurrency from others, or create new currency out of thin air.

To understand more, let's go over how we might perform a 51% attack (hypothetically, of course). To initiate a 51% attack, we need to "fork" the blockchain, which means splitting it in two. Then we need to convince the network that our malicious forked blockchain is the real one. But there is a problem: Cryptocurrencies need to have a way of knowing which blockchain is the 'real' one. Working this out is very simple – the longest one wins. By going with the longest blockchain on the network, the network can always be sure that the current blockchain is what the majority of the mining power wants. The longest blockchain being the *real* one has some other benefits too. For example, cryptocurrencies are often community driven. If the community does not like a particular update, miners won't switch to the new software. If miners don't switch to the new software, the old chain continues and remains the *real* blockchain for the network.

Essentially, to perform a 51% attack, we need to keep our fork secret. We can keep our fork either secret to one computer, or let it go between the nodes we control. Once we have our fork, we need to keep it up to date with the rest of the network. Essentially we create a mirror image of the original blockchain. You can think of our secret blockchain as a reset button. Once we have it, we can do something on the live blockchain and not copy it into our secret one. Then, we can mine a bit harder on our secret blockchain and have it be a little longer than the real one. That's why we need 51% of the hashing power on the network. Nodes in a cryptocurrency network always follow the longest chain, as it usually indicates what the network at large wants to do. Once we release our secret blockchain to the network, all the nodes grab it and see it as the *real* one, as it is the longest. And once our blockchain is the *real* one, whatever we did before is undone. Often the thing undone in 51% attacks is a transaction. We can pay for something and then switch out the old blockchain with our secret one where the cryptocurrency is instead transferred to a different address. This is referred to as a double spend. The network will reject the original transaction, as it will occur after the new transaction from the perspective of the new blockchain.

The attack does not give us the power to do whatever we want. We must still follow the rules on the network. If we don't follow the rules, our new blockchain is rejected by the network, and the attack fails. The requirement to following rules makes for an interesting combination of what we can and can't do during the attack.

An Attacker can:

Cause double spends

Collect block rewards and cause other miners to have invalid blocks

Stop transactions for a time, or remove confirmations from being added to the blockchain

An Attacker can not:

Steal cryptocurrency from others

Create cryptocurrency out of nothing

Completely stop a transaction from occurring