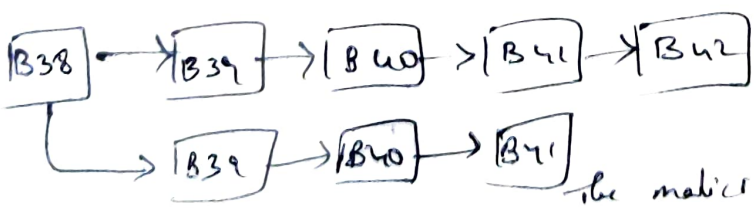
51% of attack

A 51% attack or double-spend attack is a miner or group of miners on the blockchain trying to spend their crypto's on the blockchain twice.

when a bit coin owner signs off on a transaction, it is put into a local pool of unconfirmed transaction. Miner select transaction from these pools to form a block of transactions In order to add a block of transaction in blockchain, they need solve a very difficult problem this requires a high computational power. this is called hashing. The more computation power the faster to solve it before other miners do. if it is solved it is published / broadcasted to the other miners. & they will verify it if all the transactions inside the block are valid according to the existing record of transactions of the blockchain.

Stealth mining - creating an off spring of the block

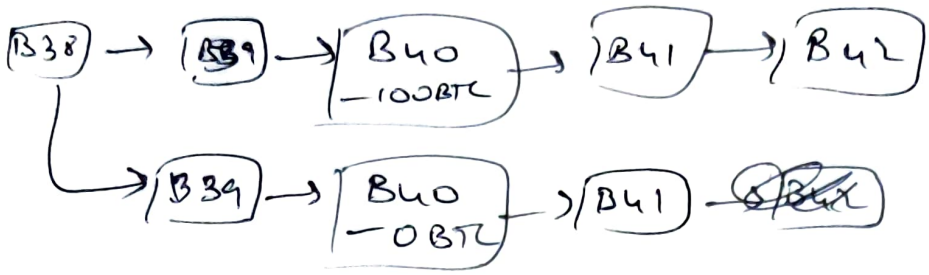
A malicious miner try's to reverse the existing transactions. When they find a sol. they need to broadcast to all the miners so that we can verify it then it can be added to the chain. However the corrupt miner can create an offspring of the blockchain by not broadcasting the sol of his blocks Thus are now two version of the block chain



truthful miners are adding blocks the chain by broadcasting them

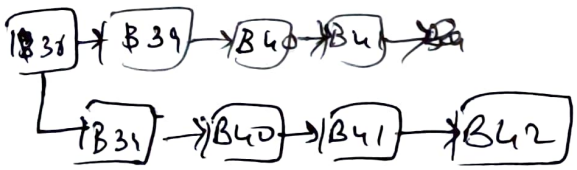
the malicious adding block to his pvt but is not broadcasting the sol to the public blockchain

if he spent 100 BTC the transaction is present in public block chain But he doesn't add that transaction in the pvt block chain he still has those coins.



Public / truthful miners mine the blocks slowly where as malicious miners mines the block almost speed because it follows the model of democratic governance i.e majority ~~the malicious miner votes the block~~.

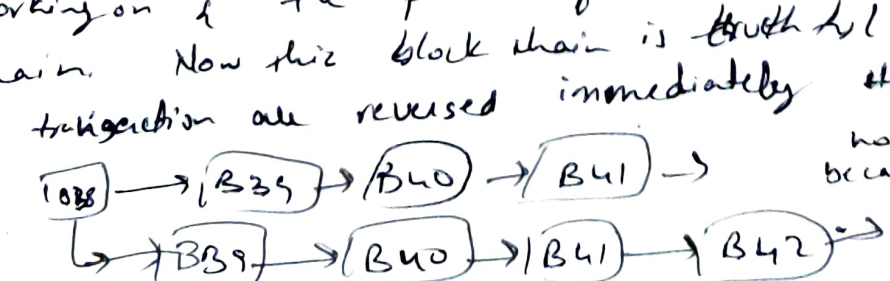
this is how all the balances of wallets are based on. whoever has the most hashing power will add block to the blockchain faster.



Truthfull miners are adding blocks to the public chain but considers very slowly than malicious miner.

The malicious miner is adding blocks to his pvt blockchain faster.

The corrupted miner successfull added the blocks in isolated Blockchain. As soon as Blockchain is longer than the public Blockchain, the corrupted miner Broadcasts this version of Blockchain to the rest of the n/w suddenly the rest of the n/w will detect the version of the block is longer than the one they are working on & the protocol forces them to switch to this chain. Now this block chain is truthfull block chain & all the transaction are reversed immediately the spend the money again



no miners there because of protocol.

The malicious miner once again spend this BTC again