Double-Spending

What Is Double-Spending?

- Double-spending - risk – cryptocurrency
- Information within a blockchain can be altered if specific conditions are met.
- The conditions allow modified blocks to enter the blockchain - reclaim

How

- Double-spending occurs when someone alters a blockchain network and inserts a special one that allows them to reacquire a cryptocurrency.
- Double-spending can happen, but it is more likely that a cryptocurrency is stolen from a wallet that wasn't adequately protected and secured.
- Many variations of attacks could be used for double-spending—51% is one of the most commonly cited attacks, while the unconfirmed transaction attack is most commonly seen.

Understanding Double Spending

Review how the blockchain works first.

When a block is created,

- hash
- a timestamp
- information from the previous block
- transaction data.

- A security protocol like the SHA-256
- Block's information is verified – closed
- New one is created with same details
- A Bitcoin is awarded to the miner whose machine verified the hash.

Understanding Double Spending

- Double spend, a secret block has to be mined that outpaces the creation of the real blockchain.
- Introduce that chain to the network
- Network would recognize it and add it to the chain.
- The person that did this could then give themselves back any cryptocurrency they had spent and use it again.

Preventing Double Spending

- Double spending -risk; minimized by the blockchain.
- The likelihood of a secret block being inserted into the blockchain is very slim – verified by miners
- The intentions of inserting an altered block is to attempt to get another user to accept a transaction using their secret block and cryptocurrency.
- The blockchain and consensus mechanism move so quickly - modified block -outdated before it was accepted.
- Even -accepted, the network - still - passed -information - reject it.

Preventing Double Spending

- Cryptocurrency transactions take some time to verify because the process involves randomly selecting numbers to solve the complex hash
- Difficult to duplicate or falsify the blockchain because of the immense amount of computing power needed to stay ahead of all of the other miners on the network.

THANK YOU!!!