Cryptocurrency Glossary

Brush up on the terms and concepts associated with cryptocurrency

51% Attack

- [ ] When over half of the computing power of an organization is controlled by one individual or a small close group of individuals, which gives them absolute rule over the organization

Address

- [ ] A bitcoin address is identical to the bitcoin owner's home address, and is visualized as a combination of alphanumeric characters (ex: 2MSSF76hs0k2aDT7f5s3KadFS34U)

Altcoin

- [ ] Bitcoin owners refer to any other coins that are not bitcoin as "Altcoin"

ASIC / ASIC Miner

- [ ] Stands for Application Specific Integrated Circuit, and is a process by which coins are mined and at a quicker rate than with a normal desktop or laptop, and done so with a chip

Blockchain

- [ ] A data system on a digital platform used to make a ledger of transactions, specifically on de-centralized networks
- [ ] It is enabled and protected via cryptography

B

- [ ] Pages in a transaction ledger with information that cannot be altered, and is permanently stored

Block Height

- [ ] The amount of blocks stacked before the first beginning block on the chain. The beginning block always begins at zero
- [ ] The amount of blocks in a chain corresponds to a metric system of time in programming

Block Reward

- [ ] This reward goes to the individual who solves the math associated to a blcok
- [ ] If you mine a bitcoin block, you will receive 25 bitcoins

Distributed & Central Ledger

- [ ] A ledger that is distributed contains data that is shared, replicable and synchronized & spans multiple networks
- [ ] A ledger that is centralized (conversely) controlled synchronized & replicable data that is controlled by a single network or individual

Fork

- [ ] A permanent divergence in a blockchain that can occur after a 51% attack or a bug in the program

Halving

- [ ] Reducing minable rewards after a sequence of blocks (after 210,000 blocks in bitcoins)

Hashrate

- [ ] The speed at white a block is discovered and solved

Mining

- [ ] The act of discovering or solving blocks in a blockchain

Multisig

- [ ] "Multisignature" when more than 1 individual is allowed to approve a transaction

Node

- [ ] A computer device connected to the Bitcoin network

P2P

- [ ] "Peer to Peer" - focuses on decentralization in which nearly every section of the blockchain can be completed peer to peer

PoW

- [ ] "Proof of Work" originated to prevent spam emails and DDOS attacks. In bitcoin terms, this is referred to as "nonce" or "number used only once" and is a way of ensuring security, although it is

PoS

- [ ] "Proof of Stake" is an energy-conserving alternative to PoW, in the sense that it requires an individual to show ownership of pariticular money or stake rather than making the individual perfom

Public/Private Key

- [ ] Public Key is utilized by any party to encrypt a message
- [ ] Private Key is utilized in a way that only an individual or group can decode it

Signature

- [ ] Mathematical process that allows an individual to prove sole ownership over his/her wallet, coin, data, etc.

Smart Contract

- [ ] A 2-way "Smart Contract" is a blockchain-stored agreement that is unalterable and possesses particular login information (very much like a "real world" contract). Once all parties have