BLOCKCHAIN TECHNOLOGY

COMPUTER ENGINEERING

BE SEMESTER VII

PROF. SWAPNIL SONAWANE

Prepared By: Prof. Swapnil S. Sonawane

MODULE 2:

CRYPTOCURRENCY

Prepared By: Prof. Swapnil S. Sonawane

TRANSACTIONS IN BLOCKCHAIN

In a nutshell, the process of blockchain transaction consists of:

1. A node in the blockchain (P2P network) requests a transaction via a wallet.
2. The transaction is broadcasted to all the nodes in the network.
3. The transaction is validated/verified by the network using consensus algorithms, i.e. preset rules set by the specific blockchain.
4. The transaction is either accepted or rejected. If accepted, the transaction is added in a chronological order along with other transactions to create a new block of data that is sealed (hash).
5. The transaction is now part of the blockchain and is permanent and immutable.

DOUBLE SPENDING PROBLEM

The double-spend problem, a flaw that is unique to digital currencies.

Double-spending, is spending the money more than once. Just as one can copy a digital file and send it to several people, it is possible to duplicate crypto-coin or token and reuse it.

If this occurs in the blockchain network, it could not only breakdown the concept of trusted distributed ledger but also lead to inflation with fraudulent, duplicate currencies in the network

The double-spend problem is circumvented in blockchain through its consensus mechanism.

Once a transaction is confirmed, it is nearly impossible to double-spend it. The more confirmed blocks in the chain, the harder it is to double-spend the crypto.

However, it is theoretically possible to double-spend a cryptocurrency. Though rare, this can be done by the 51% attack

How Bitcoin handles the Double Spending Problem?

What happened if both the transactions are taken simultaneously by the miners?

- Suppose two different miners will pick both transactions at the same time and start creating a block.
- Now, when the block is confirmed, both participants A and B will wait for confirmation on their transaction.
- Whichever transaction first got confirmations will be validated first, and another transaction will be pulled out from the network.
- Now suppose if both A and B received the first confirmation at the same time, then there is a race will be started between A and B.
- So, whichever transaction gets the maximum number of confirmations from the network will be included in the blockchain, and the other one will be discarded.

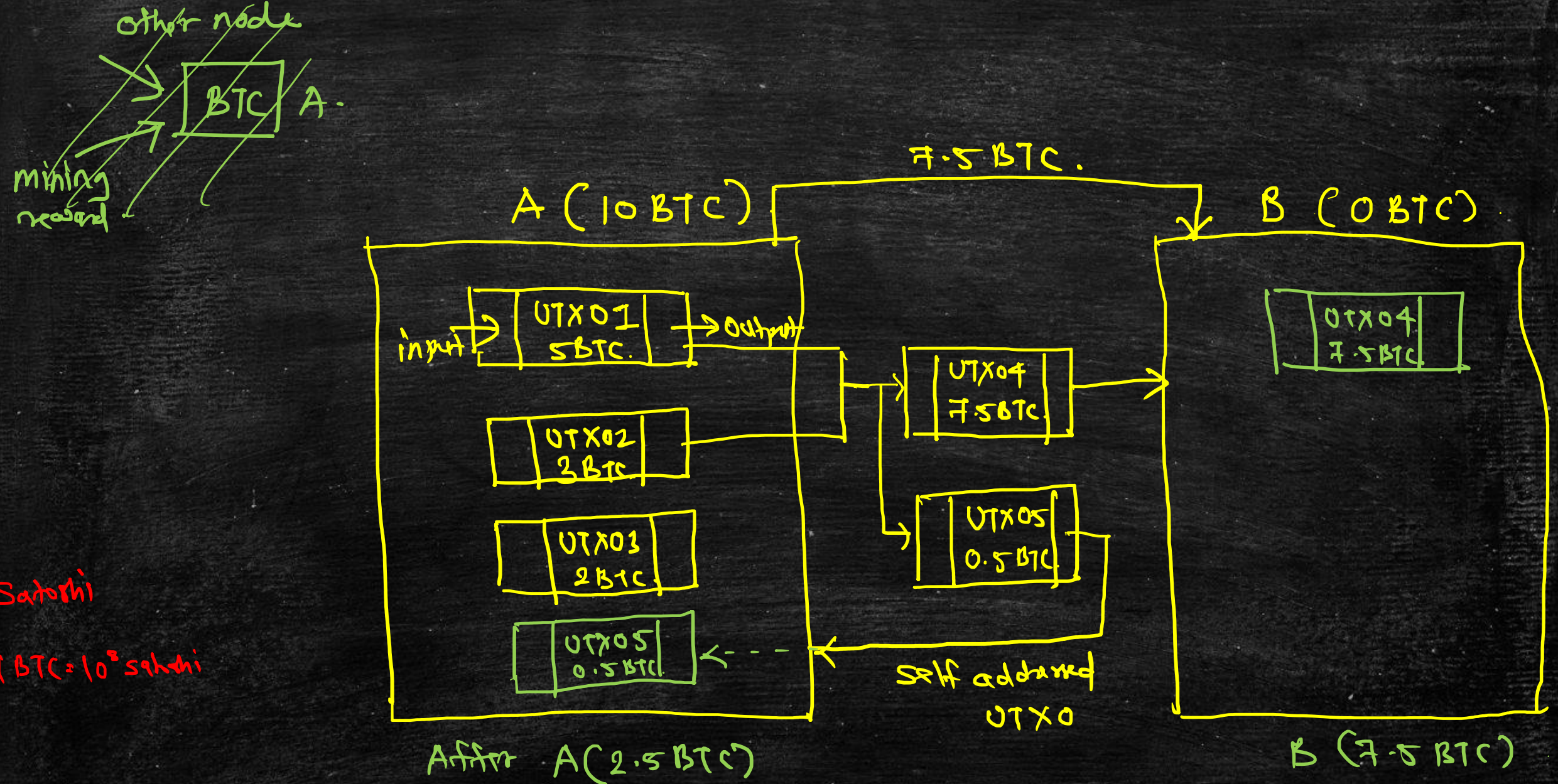
UTXO

An unspent transaction output (UTXO) is the technical term for the amount of digital currency that remains after a cryptocurrency transaction

It is the amount of digital currency someone has left remaining after executing a transaction.

When a transaction is completed, the unspent output is deposited back into the database as input which can be used later for another transaction.

UTXOs are created through the consumption of existing UTXOs. Every Bitcoin transaction is composed of inputs and outputs. Inputs consume an existing UTXO, while outputs create a new UTXO.


other node
BTC
A.
mining reward
7.5 BTC.
A (10 BTC)
B (0 BTC)
UTXO1
5BTC.
input
output
UTXO2
3BTC
UTXO3
2BTC
UTXO5
0.5 BTC
UTXO4
7.5BTC
UTXO5
0.5 BTC
UTXO4
7.5 BTC
self addressed
UTXO
After A (2.5 BTC)
B (7.5 BTC)
Satoshi
1 BTC = 10^8 satoshi

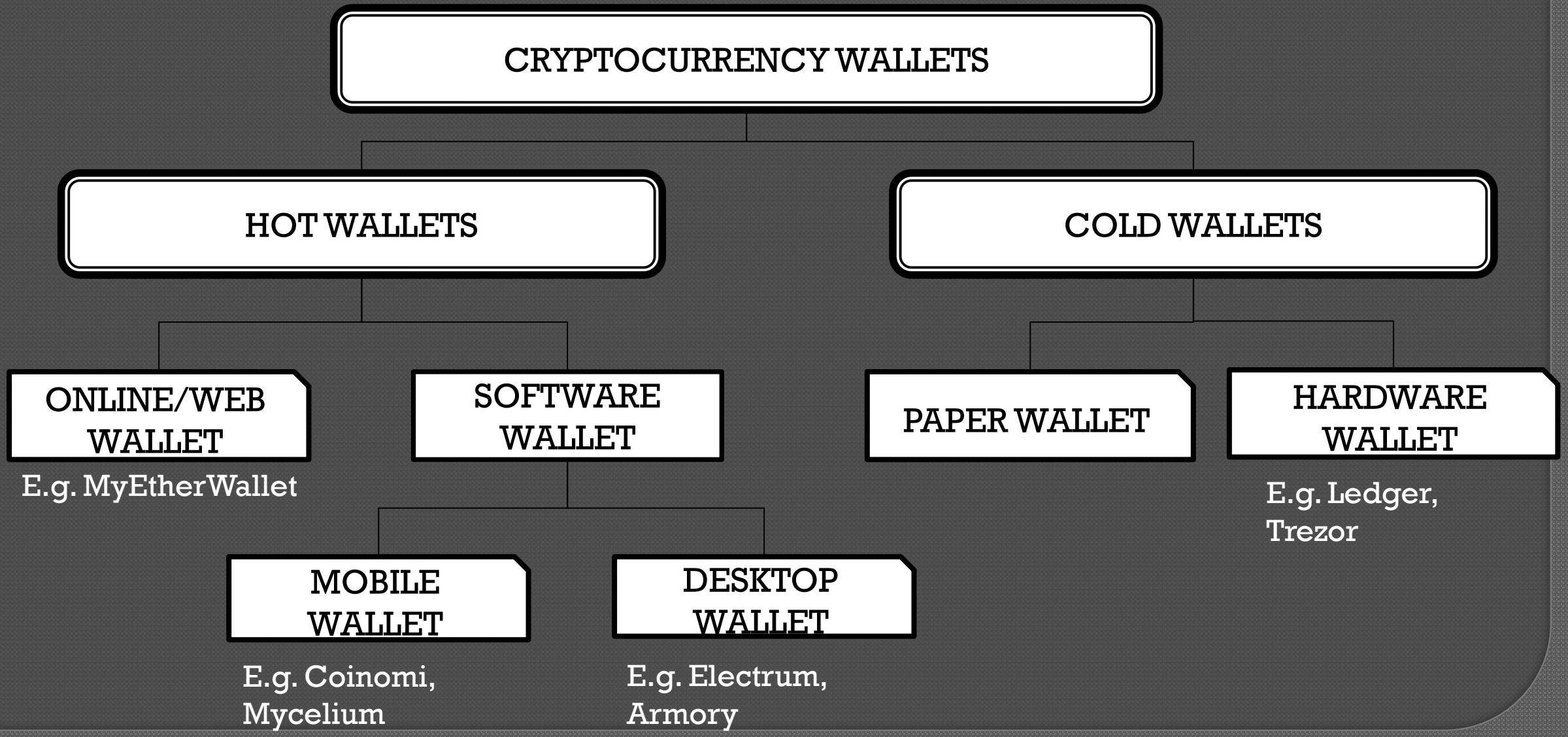
Cryptocurrency Wallets

A digital wallet or cryptocurrency wallet is a software program that stores the user's private and public keys enabling the user to transact crypto assets.

It is a management system that interacts with various blockchains to enable users to send and receive digital currency and monitor their balance.

The public key is used by other wallets to send funds to your wallet's address. However, the private key is required if you want to spend cryptocurrency from your address.

Types of wallets



Hot Wallet:

It is designed for online day to day transactions. It is connected to the internet at all times.

It is not advisable to use a hot wallet for long term storage. Hot wallets are typically free, easy to set up and convenient to use

Desktop wallet:

Desktop wallets can be downloaded and installed on our desktop or laptop. As they are locally stored, the user has complete control of the wallet.

The wallet is dependent on the security features installed on your computer.

Mobile wallet:

Mobile wallets are designed to operate on smartphone devices.

you can easily carry it with you wherever you go and make purchases from merchants who accept cryptocurrency payments using QR codes.

However, they are more vulnerable to malicious apps and viruses than desktop wallets.

Online wallet:

Online wallets are also called web wallets. They run on the cloud, and hence the user does not need to download or install any application.

They can be accessed from any computing device via a web browser.

Online wallets are hosted and con trolled by a third party and hence are the most vulnerable.

Cold Wallet:

A cold wallet is a digital wallet that is not connected to the internet. Being offline, they are more secure and used for long-term storage of cryptocurrencies.

Hardware wallet:

Hardware wallets are physical, electronic devices that use Random Number Generator (RNG) to generate the public/private key that is stored in the device.

It connects to the internet whenever the user needs to send or receive payments and dis connects once the transaction is executed.

Hardware wallets have the facility to generate a PIN to protect the device as well as a recovery phrase in case the wallet is lost.

Though more secure than hot wallets, they are less user-friendly and difficult to access.

Paper wallet:

Paper wallets are offline and, as the name suggests, it is a piece of paper with the crypto address and its private key is physically printed out in the form of QR codes. These codes can then be scanned to execute cryptocurrency transactions.

However, a big disadvantage is that the paper wallet contains only a single public/private pair, and hence they can be used only once for the whole amount in one transaction.

ALTCOINS AND TOKENS

Altcoins:

The cryptocurrency alternatives to the Bitcoin are referred to as 'Alternative Cryptocurrency Coins,' abbreviated as Altcoins or simply Coins.

Many of the altcoins come from a fork of famous and durable cryptocurrencies like Bitcoin, Litecoin, and Ethereum.

While some altcoins are like their predecessors, most attempt to improve or set themselves apart by bringing in additional features or security like improved block times, different parameters, transaction management, scripting language, consensus mechanism, etc.

The main features of altcoins are:

- They are peer-to-peer digital currencies that involve a mining process.
- They possess their independent blockchain.
- They possess the characteristics of money, i.e., they are fungible, divisible and have limited supply, and typically meant to operate only as a means of payment.

Tokens:

Tokens represent an asset, or a utility created on an existing blockchain. They represent assets that are tradable and fungible.

Tokens are used for fundraising crowd sales; Ethereum is the most popular token platform. All tokens created on the Ethereum platform are called ERC-20 tokens.

Tokens are mostly used with decentralized applications. Developers can decide how many tokens should be created and send the tokens once created. They can pay the blockchain in the blockchain's native currency when creating the token.

Tokens are distributed and sold through Initial Coin Offerings (ICO). ICOs are used to fund the development of the project. Tokens are also used for transactions on the blockchain that they have been created on.

Types of tokens:

Utility tokens:

Utility tokens provide users with access to a product or a service. These tokens are in limited supply, making them rare and valuable.

Security tokens:

Tokens issued by ICOs are mostly security tokens. They are also called as Equity tokens and they represent equity in the company that issues the token.

BITCOIN MINING PROTOCOLS

Proof of Burn:

When coins are destroyed on the blockchain, it is referred to as being burned.

Technically, the coins in circulation are sent to an unspendable address, known as an eater address.

Just like in PoW consensus where the more that is invested in supercomputers and electricity, the more the chances of mining, in Proof of Burn, more the coins one burns, the more chance one gets to mine blocks.

Proof of Burn is used in Counterparty and Slimcoin.

Proof of Work:

Proof of Work(PoW) is the original consensus algorithm in a blockchain network.

The algorithm is used to confirm the transaction and creates a new block to the chain. In this algorithm, minors (a group of people) compete against each other to complete the transaction on the network.

The process of competing against each other is called mining. As soon as miners successfully created a valid block, he gets rewarded.

The most famous application of Proof of Work(PoW) is Bitcoin.

Proof of Elapsed Time:

Proof of elapsed time (PoET) is a consensus algorithm developed by Intel Corporation that enables permissioned blockchain networks to determine who creates the next block.

PoET follows a lottery system that spreads the chances of winning equally across network participants, giving every node the same chance.

The PoET algorithm generates a random wait time for each node in the blockchain network; each node must sleep for that duration.

The node with the shortest wait time will wake up first and win the block, thus being allowed to commit a new block to the blockchain.

The PoET workflow is similar to Bitcoin's proof of work (PoW) but consumes less power because it allows a node to sleep and switch to other tasks for the specified time, thereby increasing network energy efficiency.

Proof of Stake:

With proof-of-stake (POS), cryptocurrency owners validate block transactions based on the number of coins a validator stakes.

Proof-of-stake (POS) was created as an alternative to Proof-of-work (POW), the original consensus mechanism used to validate a blockchain and add new blocks.

An algorithm chooses from the pool of candidates the node which will validate the new block.

This selection algorithm of Validators or Forgers combines the quantity of stake (amount of cryptocurrency) with other factors (like coin-age based selection, randomization process) to make the selection fair to everyone on the network.

BITCOIN MINING TERMINOLOGIES

Creation of bitcoin blocks is called mining.

Mining is the mechanism whereby nodes called "miners" in the Bitcoin world validate the new transactions and add them to the blockchain ledger.

The first miner to create the winning hash will receive rewards in the form of transaction fees or new bitcoins.

This process of computing the hash is called proof-of-work or consensus mechanism and it provides integrity to the blockchain.

All nodes in the network could participate in mining and earn mining rewards.

Block Frequency

Bitcoin transactions are being registered into blockchain once in ten minutes. Miners will first check the transaction. After reviewing the transaction, the software will give a complex target hash for the miners to solve. If miners can solve the hash, then the computer will give bitcoins as a reward to the miners.

Industrial Mining

When all the nodes are of uniform size and power, every node gets equal opportunity. It is a fair competition to get a reward. However, there are some nodes, which do industrial-sized mining and connect to a massive set of computers, consume enormous power, and use complicated software.

Mining Pool

To counteract the high time and energy consumption in transaction validation, some miners group together in mining pools to combine their mining resources for more efficiency and savings. Miners do not work for themselves; they work together in mine pooling. They share the mining power and processing power.

Halving Policy

Block frequency and Halving are the monetary policies of bitcoin. Nowadays, miners get 6.25 bitcoins as a reward to solve the hash. From the year 2009 to 2012, 50 bitcoins were given as rewards. The reward will be reduced to half for every four years. At last, in 2140, it will decrease to zero.

Block

Each block (of transactions) has three necessary informations, namely:

1. Block header
2. Hash of previous block header
3. Merkle root

Block header:

In a bitcoin blockchain, the hash function of the previous block header is stored as a reference in the next subsequent block to ensure the blocks are correctly connected.

Hash

A hash function can be considered equivalent of fingerprint of a data, similar to a fingerprint of a person. Using a fingerprint, we can identify a person since it is unique. A hash function converts the data of arbitrary size to data of a fixed size.

Merkle root

A Merkle root is the fingerprint of all transactions in the block. It is created by hashing together pairs of Transaction IDs to give a short and unique fingerprint for all the transactions in the block

Orphaned block

Detached or orphaned blocks are valid blocks, which are not part of the main chain. They occur naturally when two different miners successfully mine at the same time.

Timestamp

Timestamp is another field, which indicates UNIX time. It is the seconds passed after the first of January 1970 and is a 10-digit number. This is also part of the data, which changes every second. When the timestamp changes (every second), the corresponding data changes, as do the results.

Mempool

Blocks are added every 10 minutes, but transactions happen all the time. Mempool is the staging area for the transactions. A mempool can have around 10,000 transactions at a time. When a miner successfully mines, a set of transactions are added from mempool to the block, and into the blockchain. Once the transactions are added to the blockchain, the same set of transactions is removed from the mempool.

Block Propagation

When a miner announces a block, the block needs to propagate to all the nodes in the network, using gossip protocol. A node would perform the following functions:

a. Validate transaction

b. Make sure the nonce is valid (nonce is within an acceptable range)

c. Check if each transaction in the block is valid.

If all of the above three conditions, namely, a, b and c are valid (True), then the block is eligible for further propagation within the network; if the conditions are not met, the node will discard the block. Hence, the block would not be propagated further.

SEGWIT

The size of the signature and public key is so large within the transaction that it occupies more than 60% of the overall size of the transaction. In the bitcoin protocol, this portion (signature and public key) is kept out of the block and is distributed separately. This segregation of the signature from the block is called as Segregated Witness (SegWit). Because of SegWit, more (almost double) transactions can be added into the block. Seg Wit will be sent separately in the network.

Nonce

Nonce is a number that can be used just once in the cryptographic communication. Adding a nonce to a transaction's identifier makes it additionally unique, thus reducing the chance of duplicate transactions.

MINING DIFFICULTY

Mining difficulty refers to the difficulty of solving the math puzzle and generating bitcoin.

Mining difficulty influences the rate at which bitcoins are generated.

Mining difficulty changes every 2,016 blocks or approximately every two weeks.

The difficulty level for mining in March 2022 was 27.55 trillion. That is, the chances of a computer producing a hash below the target is 1 in 27.55 trillion.

Bitcoin mining difficulty is calculated with various formulas. However, the most common one is: Difficulty Level = Difficulty Target/Current Target.

The Difficulty Target is a hexadecimal notation of the target hash whose mining difficulty is 1.

In contrast, the current target is the target hash of the most recent block of transactions. When the two values are divided, it yields a whole number which is the difficulty level of mining bitcoin.

An adjustment of difficulty upwards or downwards depends on the number of participants in the mining network and their combined hash power.

The mining difficulty of a cryptocurrency such as Bitcoin indicates how difficult and time-consuming it is to find the right hash for each block.

MINING POOL

When all the nodes are of uniform size, power, and every node gets equal opportunity, it is a fair competition to get a reward. However, some nodes indulge in industrial-size mining, by connecting to a massive set of computers, consuming enormous power, and using complex software.

It will be difficult for individual miners to compete with them.

To counteract the huge time and energy consumption involved in transaction validation, some miners group together in mining pools to combine their mining resources for more efficiency and savings. They share the mining power and processing power.

Mining pools provide the service; they share the services so that the individual miners do not repeat the work, thus avoiding double work and waste of time. Nonce values (cryptographic puzzles) are distributed among the individual miners within the pool.

When one of them finds the golden nonce, the corresponding mining pool wins the reward for that block. They share/split the reward based on the computing power (hash rate) of the individual miners.

However, mining pools can go against the basic principle of distributed ledgers as someone or a group gaining control of over 50% of the computing power of the network, usually referred to as a 51% attack, can control the validation process.

51 % attack is not designed to tamper with the blockchain. In order to attack a block within the blockchain, the hacker needs to change all the subsequence blocks of the blockchain