Block: Block is a data structure that stores a bunch of transactions and submits them to the Blockchain for validation. If validation is successful, the block becomes immutable.

The Miner Node generates blocks. Miner Node picks uptransactions from the memory pool and generates a block. This block is also called "Candidate block."

Every block consists of the following:

Block header: Contains version, last block, time, and target

Nonce: Number to consider for hash generation

Transactions: List of transactions in a Merkletree format

Block header consists of critical information such as version number, last block hash, timestamp, target number, and so on.

The block is added in the chain by hashing the block header and hoping that data is less than the target number.

A nonce is a number that is used by the miner to generate the hash to meet the target number. The Nonce is incremented by the miner to meet the required target value.

Once the hash is found, the block is mined and submitted to the chain. Each block is linked with the previous block, forming the chain.

Chain The chain is the blocks linked together using cryptography and shared across every node.

A hash that links one block to another, mathematically “chaining” them together. This is one of the most difficult concepts in blockchain.

The hash in blockchain is created from the data that was in the previous block. The hash is a fingerprint of this data and locks blocks in order and time.

Since the chain is distributed across the network, there is no chance of fraud. If someone tries to add a false block from their machine, the network will verify and reject the block. To take over the network, one must have 51% control of the node (Hashing/Computing power of the node) in the network.

It is also called a 51% attack.

Hashing is a one-way function that cannot be decrypted. A hashing function creates a mathematical algorithm that maps data of any size to a bit string of a fixed size. A bit string is usually 32 characters long, which then represents the data that was hashed. The Secure Hash Algorithm (SHA) is one of some cryptographic hash functions used in blockchains.

SHA-256 is a common algorithm that generates an almost-unique, fixedsize 256-bit (32-byte) hash

Miners Miners are the nodes that perform the process to add a new block in the chain, adding the transactions sent by the user.

Miners do this process by performing a deep level of hash calculations that takes around 10 minutes in the case of Bitcoin.

This calculation costs a lot of computing power, so it is required to pay the miners to run the operation in the surplus profit. Every time a miner performs a successful block insertion in the chain, the system rewards them with an incentive. In the case of Bitcoin, it is 12.5 Bitcoin per successful block at the time of writing this article.

Consensus The consensus is the set of rules agreed by all parties of the network.

Blockchain Consensus algorithms ensure each new block added to the network is the only version of the truth, which is agreed by all the nodes in a distributed/decentralized computing network.

A consensus algorithm is a mechanism in computer science used to establish agreement on a single data value across distributed processes or systems. A consensus algorithm is a protocol through which all the parties of the blockchain network come to a common agreement (consensus) on the present data state of the ledger and be able to trust unknown peers in a distributed computing environment.

There are three types of consensus algorithms used by the Blockchain networks.

Proof of work

Proof of stake

Byzantine fault tolerance

if a hacker gets access to 51% or a more significant part of the network. The various types of consensus protocols solve the 51% attack problem .

Network: A network is a collection of devices or systems that are connected to each other that allows them to share resources between them.

There are broadly three different kinds of network as highlighted in the diagram:

Centralized network: — In case of a centralized network, we have a central network owner. The central network owner is a single point of contact for information sharing. The biggest issue with a centralized network is with a single central owner it also becomes a single point of failure. Further, with a single copy stored with the owner, every instance of access to the resource leads to an access issue with time.

Decentralized network — As for the decentralized network, the we have multiple central owners that have the copy of the resources. This eliminates the biggest problem of single point of failure with centralized network. With multiple owners, if a particular central node fails, the information can still be accessed from the other nodes. Further, with multiple owners the speed of access to the information is also reduced.

Distributed network — The distributed network is the decentralized network taken to the extreme. It avoids the centralization completely. The main idea for the distributed network lies in the concept that everyone gets access, and everyone gets equal access.

The blockchain makes use of the distributed network, such that everyone downloads and interacts with all the information that is available on the Blockchain. The need for this arises from the core concept of having a completely decentralized system with no dependency on a 3rd party system. Further, having complete access ensures that one does not need to depend on anyone else for any help.

Channel Link: https://www.youtube.com/channel/UCrnG1hqq6GhLO7MmndzBA-w

KMC102/202

EMERGING TECHNOLOGY FOR ENGINEERING

UNIT - 3.3

By PyIntern

PYINTERN

Online Training Institute