Blockchain

Concept given by: Stuart Haber & W. Scott Stornetta (1991)

Characteristics of Blockchain:
1. Hash Cryptography
2. Immutable Ledger
3. Distributed P2P Network
4. Mining
5. Consensus Protocol

Hash Cryptography:

Cryptographic hash function is an algorithm that converts any form of data into a unique string of text.

SHA256 (Secured Hash Algorithm , takes 256 bits of memory) : 64 characters, hexadecimal number

Requirements of Hash algorithm:

1) One way (we cannot recover data with the given hash, same as we cannot detect person with the given fingerprints)
2) Deterministic (same hash value every time for a particular document)
3) Fast computation
4) The Avalanche effect (if we make even a small change in document, hash value will be completely different)
5) Must withstand collisions

Immutable Ledger:

In block chain, data in an existing block cannot be changed as small change in the data will change the hash function of that block completely. In order to make changes, we have to make changes or we can say we have to mine all the blocks which comes after the targeted block as the next block contains the hash of previous block also which will create discrepancy if not mined again. This whole process will take huge computational power which is almost impossible to get.

Distributed P2P Network:

Peer to peer network is known as decentralized network that consist of group of devices that collectively stores and share files without any central administration or server. In blockchain, this architecture allows all cryptocurrency to be transferred worldwide, without the need of any middle-man or central server.

Consensus Protocol:

Consensus protocol help all the nodes in the network verify the transactions. Consensus protocols are of different types such as: POW(proof of work), POS(proof of stake), PoSpace(Proof of space), PoET(Proof of Elapsed time). Bitcoin uses POW for verification on all nodes.

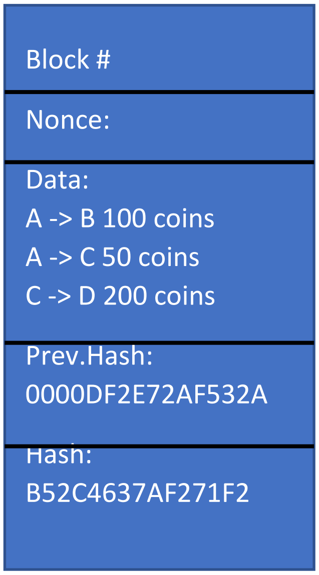
POW: Miners perform computational work in solving mathematical problem to add the block to the network. (Bitcoin and Litecoin uses POW)

POS: A person can mine or validate block transactions according to how many coins they hold. (Ethereum uses POS)

PoSpace: It is similar to POW. Instead of computational power, PoSpace uses disk storage to validate transactions. Also known as Proof of capacity. (Burstcoin, Chia and Spacemint uses PoSpace)

PoET: Developed by Intel, PoET consensus is an efficient form of proof of work that removes the need for the mining-intensive process and replaces it with a randomized timer system for network participants. Basically, each network participant is given a random timer object and the first timer to expire “wakes up” that participant who becomes the block leader and produces the new block.

Mining:


Block #

Nonce:

Data:
A -> B 100 coins
A -> C 50 coins
C -> D 200 coins

Prev.Hash:
0000DF2E72AF532A

Hash:
B52C4637AF271F2

Structure of a block

First block is called Genesis Block and it has no previous hash value.

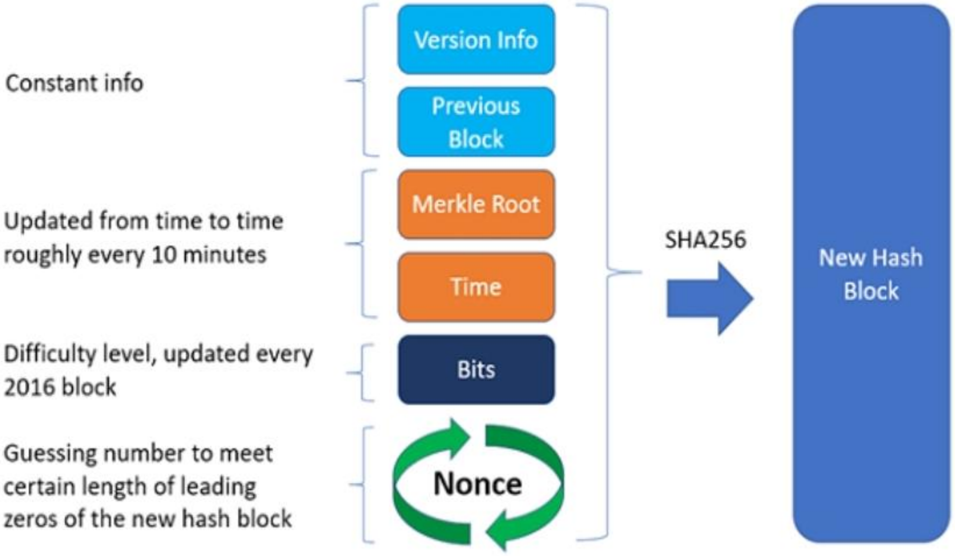
How does mining work???

Miner's goal is to add block to the blockchain by solving a mathematical problem.

Miners take few inputs from the block which are:
Version info, Previous block hash, Merkle root, Timestamp, Difficulty level bits and combine Nonce with this information.

Version info: It indicates which set of block validation rules to follow.
Previous block hash: Hash value of previous block.
Markle root: It is made up of all the hashed transaction hashes within the block, ensuring that none of those transactions can be modified without modifying the header.
Timestamp: It is the time when miner started hashing the header. Must be strictly greater than the median time of the previous 11 blocks. Full nodes will not accept blocks with headers more than two hours in the future according to their clock.
Difficulty level: The target hash value. Bitcoin algorithm is programmed to self adjust the difficulty level every 2016 blocks, roughly every two weeks.

Nonce (Number only used once) : An arbitrary number miners change to modify the header hash. Nonce is a number added to a hashed or encrypted block in a blockchain that when rehashed meets the difficulty level restrictions. Nonce is the number that blockchain miners are solving for in order to receive cryptocurrency.


Constant info
Version Info
Previous Block
Updated from time to time roughly every 10 minutes
Merkle Root
Time
Difficulty level, updated every 2016 block
Bits
Guessing number to meet certain length of leading zeros of the new hash block
Nonce
SHA256
New Hash Block

So, miners goal is to take Version info, Previous block hash, Merkle root and Timestamp as input and get a hash value less than the difficulty level. As, all these four values are constant, Nonce is used which is an arbitrary number miners change to modify the header hash to produce a hash less than or equal to the target threshold (difficulty level). In bitcoin, nonce is 32-bit value.

Some points to be noted:

* If anyone try to attack any particular block in blockchain and make changes to it, hash value of that particular block will change and therefore, discrepancies will be there as block also contains hash value of previous block. So, in order to make changes, attacker has to update all the following blocks which is nearly impossible. In case, if someone succeed in making changes to all blocks, it will be

rejected as blockchain for all other peers will be different and they will reject the chain in minority.

* If two different blocks are added to different peer’s chain, which one will be valid??

Here comes the role of Proof of work. Both will be on hold till the next block will come. During the next block addition, whoever has the high computational power and solve the next puzzle early, his chain will be valid. And the other transaction will be invalid. Therefore, it is said that for a transaction to be valid, wait for few more blocks following that.

Palak Jain