What is Blockchain?

A blockchain is a distributed ledger that basically holds a list of records in semi-ordered manner. A copy of this list exists at every computer within the Blockchain network. In this project, we are interested in the technical details and use cases of this new technology.

Blockchain could be public or private. It depends on the crypotcurrency, but in Bitcoin, the blockchain is public. In blockchain, every block has many transactions which contain key information like amount, sender, receiver (in our Bitcoin case).

Every block has a header which holds “Merkle Root” and “Hash of previous block header” and every block has a list of transactions within it's body.

In header, hash of previous header is there for making sure that block is not altered. When someone changes the previous block, its hash value changes which affects all the chain and makes the malicious activity visible to anyone.

Merkle root is a sort of signature of transactions within that block’s body part.

Here, when someone changes a transaction it would change specific hashes and it will result in a different Merkle root and which makes blockchain unchangeable.

Hash of the previous block, Merkle root and nonce must be smaller than the target.

MINING PROCESS

Miners are people that are trying to find a “Nonce” that satisfies that given target. It could be assumed as throwing darts blindly tossed. While you are blindfolded, trying to hit any place is equally likely but if you throw faster, you can hit the target faster. In Bitcoin, if you have superior hardware, you have the advantage in this challenge. Miners are earning bitcoin by verifying the blocks.

What is Bitcoin?

Bitcoin is a kind of cryptocurrency which exists purely in the digital realm first time used in 2009. It born out of the Cypherpunk movement, a libertarian struggle for privacy and self-governance. Invention of Bitcoin inspired the creation of Ethereum by Vitalik Buterin who is an anonymous identity.

What does Bitcoin provide?

- Account and Identity management: Every user has an address and each of them relevant with amount of currency.
- Services: Users can do transactions between each other via other users.
- Record management: Redundant information is stored by users which are on the system via a blockchain.
- Trust: Trust comes from personal encouragement aligning with community goals.

Some History of Bitcoin

- $74 million = 2 Pizzas
- bitcoin is the most valuable crypotcurrency today.
- Before the Bitcoin gets valued, there was a trade which a guy bought two pizzas for 10,000 Bitcoin, today it's value is ~$4 million.
- Bitcoin Theft
  - Mt. Gox was the biggest online bitcoin exchange market. More than 1% of transactions were being occurred via Mt. Gox. In 2014, Mt. Gox lost 744,408 bitcoins in a theft, then Mt. Gox declared bankruptcy.
- Bitcoin in Illegal Use
  - Due to Bitcoin anonymous protocol, it is used in the black market for illegal goods. Silk Road was one of them, it was sold goods for Bitcoin via Tor network.
  - It was shut down by FBI with seizing $3.5m in Bitcoin.

Ethereum design based on the following 5 principles:

- Simplicity: Ethereum protocol should be as simple as possible to protect over data storage or time efficiency.
- Universality: Ethereum provides its own script language which developers can use to create contract or transaction type.
- Modularity: Ethereum created as possible as modular and separable.
- Agility: There is the opportunity to make the change on high-level constructs
- Non-discrimination and Non-censorship: Ethereum protocols should prevent to attempt any restriction and any discrimination which come from central authorities.

Ethereum is a decentralized platform that uses smart contracts to run applications on a custom blockchain. This blockchain has powerful associated global connections that can share valuable items and contain ownership of possessions.

This features give opportunities to create markets, store given promises or record of changes, make action with funds based on instructions given in past and many different things that have not been think about yet.

Vitalik Buterin is a developer from Toronto who is the creator of Ethereum. He focused on the blockchain, crypto technologies and Bitcoin in 2011. Then, he came up with an idea of a platform that gives the opportunity to develop other decentralized application beyond the financial usage with the smart contract.

Puregold

Puregold is a cryptocurrency idea that was designed by team and supervisor in order to research the common uses of blockchain and cryptocurrencies and implement a version for in-campus usage.

Puregold rewards a discount for in-campus purchases with respect to currently stored puregold count in users account. This idea was designed to raise awareness about blockchain in general.

What is Ethereum?

Ethereum is an open-source platform that allows developers to write applications or contracts on the blockchain. It is built on top of the Ethereum Virtual Machine (EVM), which is a virtual machine designed to run on any computer with sufficient computing power.

Ethereum supports a programming language called Solidity, which developers can use to write smart contracts. These contracts can be executed on the blockchain and can interact with each other, allowing for the creation of decentralized applications.

Transaction and Messages

Basiclly, transactions are data packages that generated and signed by external owned accounts and includes message, then submitted to blockchain. All transactions contain:

- nonce: count of number of transactions sent by sender.
- The recipient of the message
- The address of the sender
- The amount of the ether to transfer
- Optional data field
- The maximum amount of the gas that sender will pay to execute transfer
- Gas price

In Ethereum, transactions can be sent using either the native Ethereum token, Ether, or any other ERC-20 compliant token. Transactions can also be relayed using external callback, which is a service that monitors the blockchain and can execute code on the blockchain when a specific transaction is detected.

Identity

With identity, people can receive, claim, spend the Bitcoin. Identity provides a random private key, then public key is created corresponding private key. Public key is for receiving money, private key is for accessing the account to manage.

Transaction

Transaction is valid when three conditions are satisfied:

- Proof of ownership: There must be a signature of ownership.
- Available funds: Users must have enough amount of Bitcoin.
- No double spending: Other transactions can’t use the same funds.

Record Keeping: The Blockchain

Transaction ledger is stored with distributed database, everyone on the system stores the ledger.

Consensus (Proof-of-Work)

To prevent double spending, every transaction must be validated by the other peers. Bitcoin has anonymous identity, so people can have multiple accounts to take opportunities of cast vote. That is why Bitcoin validation protocol uses resources instead of cast votes. Peers use their CPU power to vote. They have voting power as much as used power. (System assumes majority of the network is honest)

Proof of Stake

Proof of Stake is the consensus protocol as an alternative to proof of work, to use consensus on which block will be the next in blockchain. Creator of next block selected by the randomized system according to how much cryptocurrency account have or how long account has been holding that particular currency rather than computational power as proof of work system.

Possible advantages of proof of stake against proof of work are that:

- It reduce to energy consumption while add the new block on blockchain.
- There is no need to create many new coins in order to encourage miner to continue mining process.
- Proof of stake more secure against 50% attack than the proof of work.

Proof of Work

Proof of Work is the consensus protocol as an alternative to proof of work, to use consensus on which block will be the next in blockchain. Creation of next block selected by the randomized system according to how much cryptocurrency account have or how long account has been holding that particular currency rather than computational power as proof of work system.

Possible advantages of proof of stake against proof of work are that:

- It reduce to energy consumption while add the new block on blockchain.
- There is no need to create many new coins in order to encourage miner to continue mining process.