Introduction to Bitcoin:

- Bitcoin is a currency. Try: in Google browser BTC/THB
- A Payment System that consists of computers live across the Internet.
- A Bitcoin Network Protocol defines the sets of rules for communication between Bitcoin nodes that connected throughout the world.

The Bitcoin Payment System just allows transferring BTC, no financial services.
It is not a bank, no office building, no employees and no owners.
Bitcoin offers service without fee but tips are welcome.
It is working 24-7 from anywhere around the world and anyone are allowed.

bitcoin.org is a non-profit organization that maintains the Bitcoin technology.

It creates bitcoin core, an open source system that regarded as the reference implementation of the Bitcoin Network System.

It continuously improves the Bitcoin technology by allow anyone to send Bitcoin Improve Proposal (BIP) to the organization.

The Birth of Bitcoin:

Satoshi Nakamoto started working on an electronic cash system around 2007.

August 2008, he registered the domain bitcoin.org and sent emails to a group of peoples exposing the idea of the project.

October 2008, he published an article 'Bitcoin: 'A Peer-to-Peer Electronic Cash System' (The Bitcoin White Paper) and exposed the initial source codes of the system.

https://bitcoin.org/bitcoin.pdf

For a couple years, he communicated extensively through emails with a group of experts and developers, collaborating their contributions to the project. The e-mails and forum posts have been saved at satoshi.nakamotoinstitute.org.

January 4, 2009, he started the first official Bitcoin Blockchain and sent the first transaction to himself, marking the beginning of Bitcoin.

By the end of 2010, he stopped communicating and vanish without a trace. There were a lot of speculation and investigation on who he is but no conclusion.

Between January and July of 2009, Satoshi created more than 1 million BTC for testing the Bitcoin system. We don't know exactly how much BTC he own, but not a BTC of his known addresses had been spend to this day.

Traditional Banks:

- Banks need customer registration, request a lot of personal information and stored customers balance, credit and financial activities.
- Customer data are stored in the bank servers with heavily protection.
- Bank transactions are processed at bank servers without any witness.
- Bank customers need to verify themselves every time to perform financial activity with their accounts.
- Banks work under government regulation rules and support.

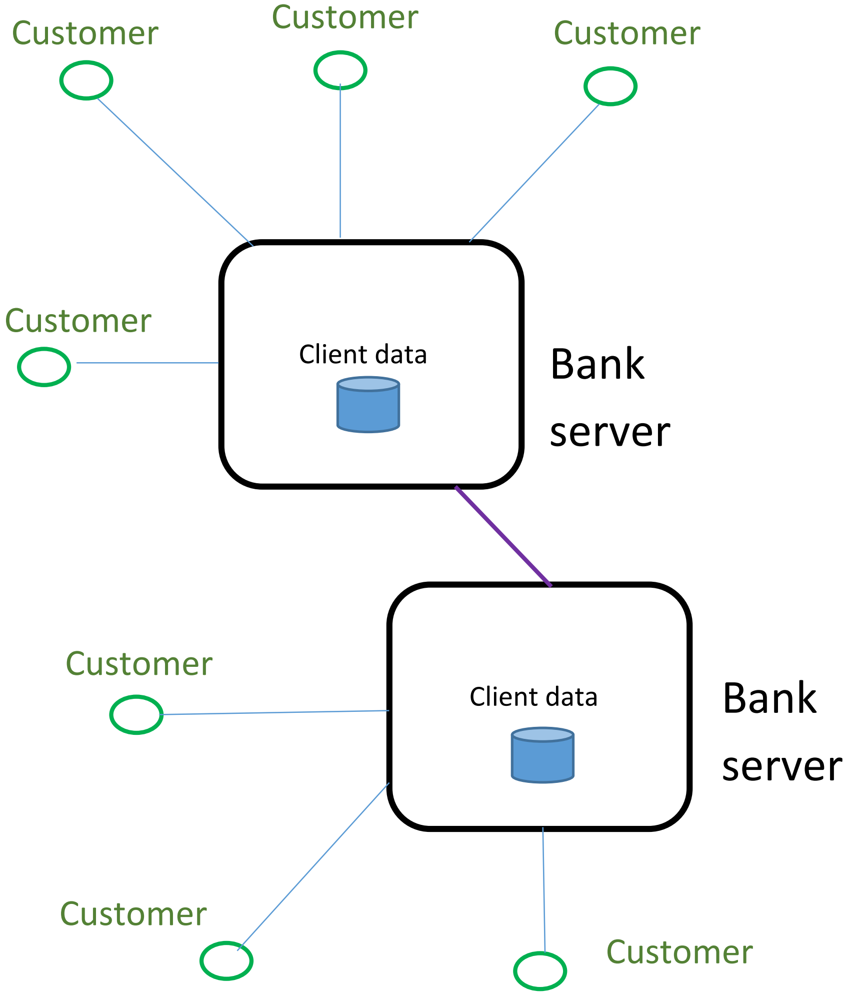
Bitcoin:

- Bitcoin users do not need registration nor provide identity information.
- User transactions are stored in Blockchain distributed across the Internet.
- Bitcoin transactions are publicly processed and verified at thousands of miner nodes across the world.

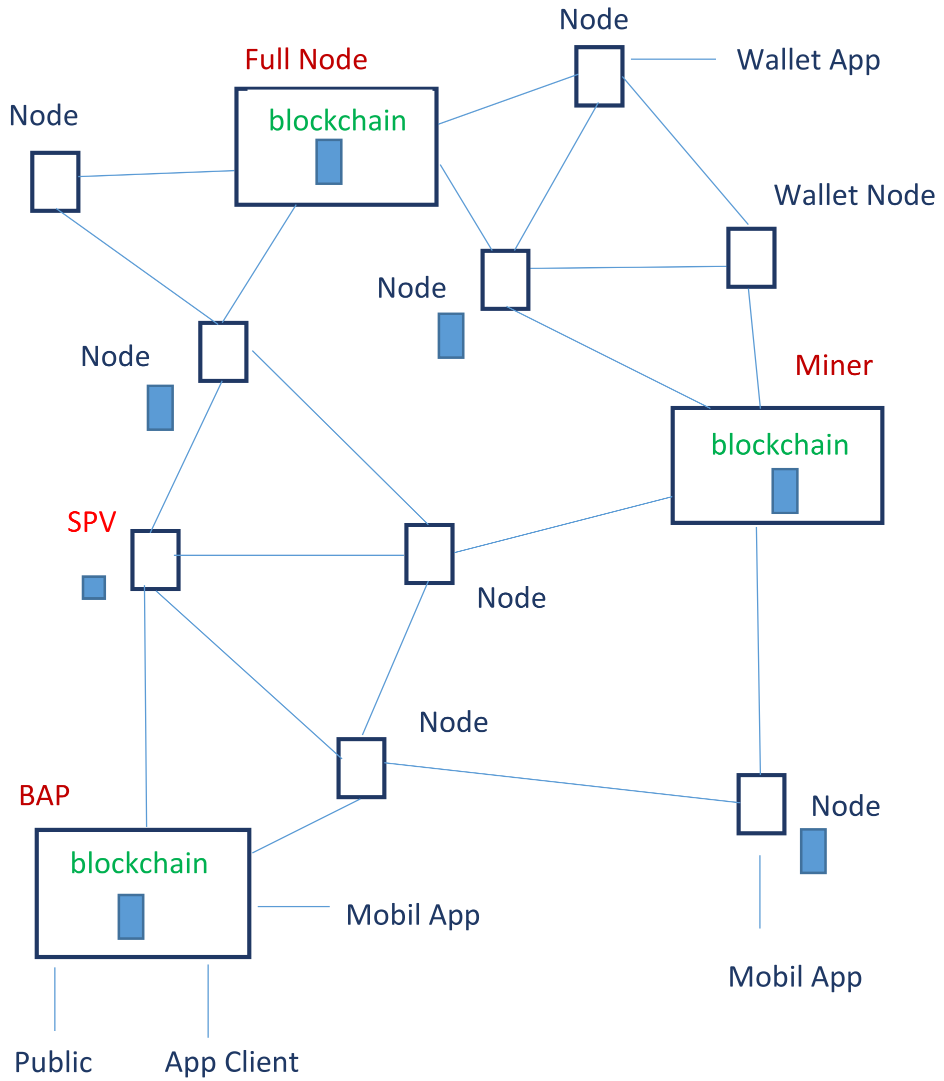
Try: blockchain.info

- Bitcoin users need just their private key to issue transactions without exposing their identity.
- Bitcoin works under the agreement and trust in the technology.

Traditional Banks



Bitcoin Network



Nodes are arbitrary connect to others, which can join and leave anytime.

Node Types: Nodes are classified by functionality:

Full nodes

- Perform all aspects of the Bitcoin protocol without external help.
- Permanently connected and store the entire Blockchain
- Normally used in organizations that intensively interact with Blockchain.

Simplified Payment Verification (SPV) or Lightweight nodes

- Provide transaction and balance services to some users.
- Occasionally connect to neighbor nodes as needed.
- Store some part of the Blockchain for specific users.
- Mostly used by financial companies to do business with Bitcoin.

Wallet nodes

- Simplify creating user account, transactions and checking user's balance.
- Store and protect user keys.
- Connect to the network as needed and disconnected after usages.
- The mostly used by Bitcoin users.
- Wallet clients are applications that connected to already exist nodes.

Miner nodes

- Participate in mining race.
- Manage and maintain its own Blockchain.
- Permanently connected while mining.
- Mostly do not provide other user services.

Bitcoin Access Provider nodes

- Provide accessing to Bitcoin network for users that do not want to maintain their own node and Blockchain.
- Permanently active and provides access through the public.
- Mostly support Json-rpc and restful API interactions.

The basic functionalities of nodes are:

wallet(W), miner(M), bitcoin(B) and network(N).

Nodes that provide all four functions (WMBN) are called 'full nodes'.

All nodes must at least have the network (N) function to discover, maintain connections and exchange messages with other nodes.

Wallets:

Most users participate in Bitcoin systems through a kind of program called ‘wallet’. Choosing a wallet is highly subjective and depends on the user.

Wallets can be categorized according to their platforms and how keys are managed:

Paper Wallets: Keys are written on paper, low-tech, offline, but perhaps more secure than other kinds of wallets.

Desktop Wallets: are programs run on desktop PC. Keys are normally saved on files in the hard disks or USB drives. But they must be properly maintained.

Mobile Wallets: are programs run on smart phones. Keys may be saved on the phone or to cloud services. The phone camera can take advantage of handling addresses as QR codes and the phone can go with the user anywhere and most of the time.

Web Wallets: are web applications. Keys are stored on the server or to a third party service. The security is compromised in exchange for software installation and keys management.

Hardware Wallets: are devices that operate as wallets, mostly in a form of USB drives. Keys are stored in self-contained memory. Very handy to go anywhere but likely to get lost or stolen.

As of November 2024, the Bitcoin Blockchain size is approximately **530 GB**.

Nodes without Blockchain can verify just the structure of transactions.

Full nodes and miners can verify correctness of transactions without external helps.

SPV nodes are designed to service a group of users without storing the entire Blockchain but request some transactions from neighbor nodes when needed.

All nodes must be able to verify transaction structure (not the user balance). So that only the valid transactions will be propagated in the network.

Bitcoin servers open two ports:

8333 for Bitcoin protocol to communication:

- Consistently maintaining connections, mostly with 4-5 neighbors.
- Propagate transactions.
- Maintaining Blockchain.
- Message exchange with other nodes.

8332 to communicate with users using HTTP protocol.

- To send transactions from users to Bitcoin network.
- To get user balance or transaction information.

Blockchain: is the storage for transactions of Bitcoin system.

Bitcoin transactions are collected into a block, and blocks are linked into a Blockchain.

Transactions

Abstract transactions.

… send 10 to John.

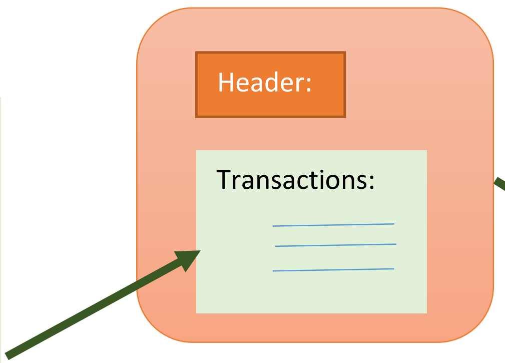
John send 2 to Jack, and send back 8.

Jack send 1 to Joe, and 1 to John.

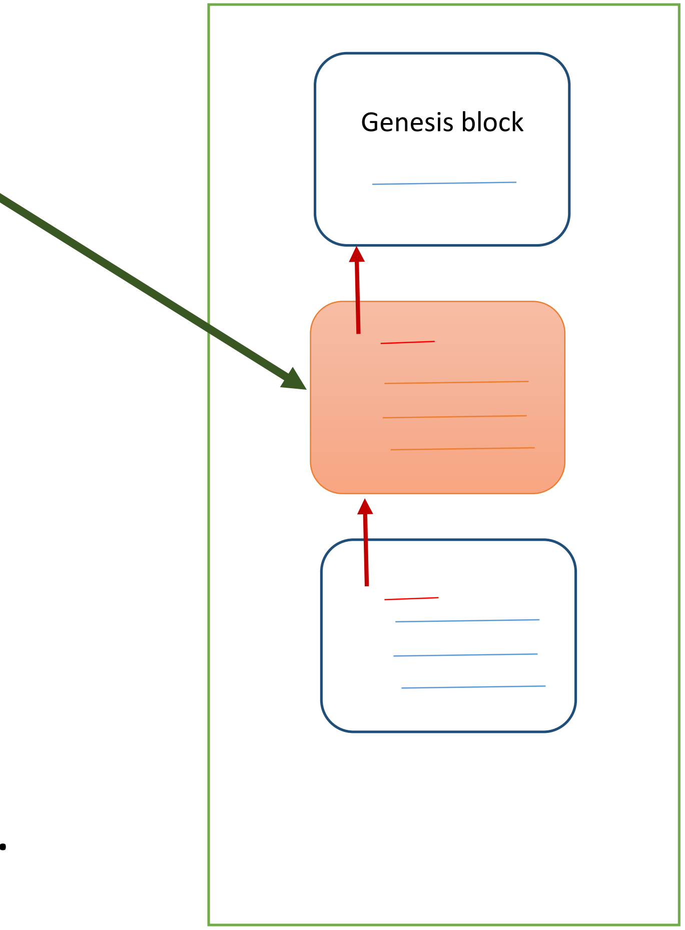
John send 3 to Jim and send back 6.

Jim send 3 and John send 6 to James.

Block



Blockchain



A transaction contains: <sender> BTC <receiver>

Sender is the one who create and send the transaction.

Receiver is the one who receive the transferred BTC.

Bitcoin Bootstrapping: The processes that a node performs when started up:

1. Read configuration, starts necessary setup processes and ports.
2. Discovers neighbors and establishes connections. Five well known seed nodes are stored in source code but allows given at startup. Last session connected nodes are remembered and try to reconnect before the seeds.
3. After connections are established, they start handshaking by exchanging messages e.g. version and IP addresses.
4. Check the existing Blockchain and catch up if needed until up to date.
5. Provide services for users.

This explain how Bitcoin network established all over the world.

Some nodes may refuse connection, e.g. if the version is not acceptable.

If no communication for a while, nodes will periodically send a message to check the connections. If a neighbor does not respond within 90 minutes, it is assumed dead and a new neighbor will be sought.

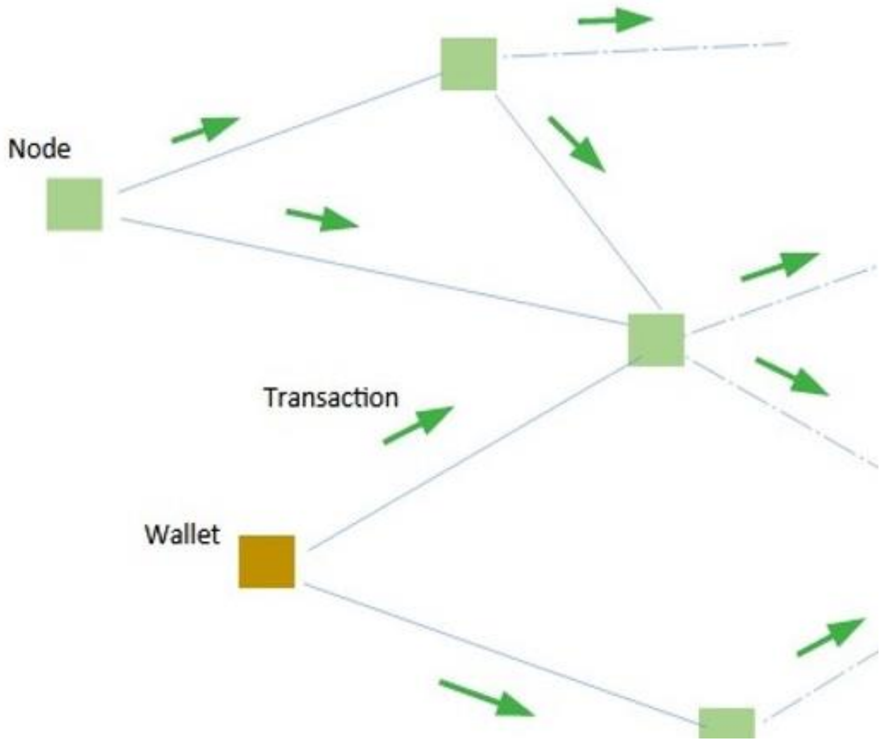
A node will be forgot if no connection for 3 hours.

Transaction Propagation:

- A transaction is created (mostly by *wallets*) and sent to neighbors nodes.

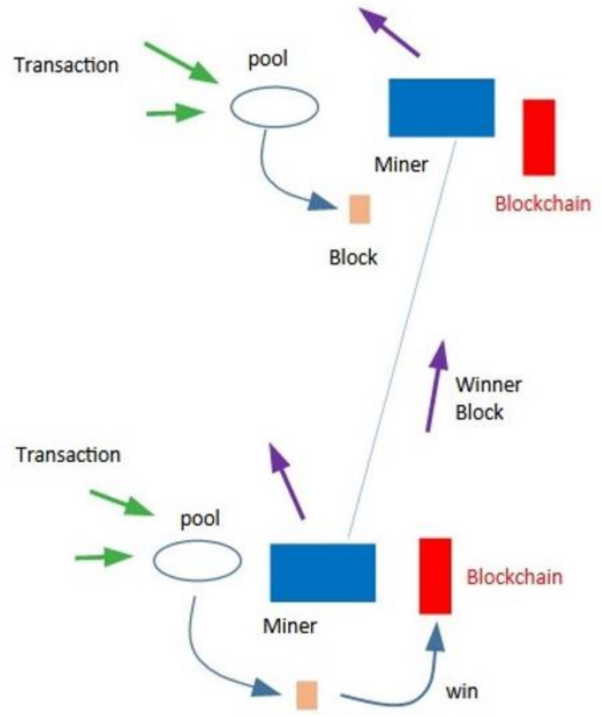
- The transaction is structural verified, not the correctness of the balances.

If valid the transaction is sent to neighbor nodes, this is called transaction propagation that makes the transaction float around the Bitcoin network.



Miner Nodes:

When a transaction arrives at a miner node it will be validated against the miner's Blockchain if valid it is put in the minor's pool. This is called publicly verification.



- In each round of racing, a miner creates a block that contains transactions from the pool while compute a resolution to the proof-of-work (will be explained later).

- If a solution is found it is included in the block and called a winning block the propagated to the network. The miner who finds a solution first is a winner.

- When other miners receive the winning block, the block is verified if valid its valid counter is increased by one then the winning block is propagated to the network.

- When the winning block has certain number of valid counter, a signal declaring a winner is send throughout the network. The racing round is over and the winning block is saved to every nodes Blockchain. Then the new round begins. That should made all nodes Blockchain the same all over the world.

Blockchain resolving:

Since transactions are propagated throughout the world, they normally arrive at miners in different time and order. Occasionally there are many winning blocks in a round in different parts of the world. And they are saved in Blockchain that conform to the winning block.

Bitcoin has mechanisms to detect the situation and automatically resolve to only one winning block which got the highest consensus this is called Blockchain resolving.

Resolving removes the unlucky winning blocks from the chain and replaces with the truly winner which is the one with the highest follower blocks. That happened all the time, but resolving deeper blocks requires modifying the chain down to the last blocks.

Since the Bitcoin is in operation, there is no more than 5 deep blocks had been resolved.

To cheat the Blockchain with your evil transactions you would need to win approximately up to 5 consecutive mining rounds which is very hard and can be detected later anyways.

A Bitcoin mining round was designed to take around 10 minutes each. When a transaction needs some time to propagate and wait in pools to the end of current round if lucky to be picked in the next round. Therefore after sending a transaction we should wait about one hour (6 blocks had been added to the Blockchain) so that the transaction is confirmed which means it is safe to be redeemed. Just always check your balance before spending.

Bitcoin Miner Incentive:

It was estimated that in 2024, there are over 5 million Bitcoin miners globally.
Bitcoin trustworthy relies on publicly verification by miners. The more miners, the more secure and robust the system. But how to seduce miners to participate in the system.

All Bitcoin blocks have the first transaction called Coinbase Transaction. It was created by the miner to transfers an amount of BTC to the miner, if wins the round as the incentive reward for performing publicly verification. That keeps the system functions without external fund.

There will be only one winner in each round who earns the incentive BTC.
So the competition is very tough while hardware technology is getting better every day. Miners must spend more and more investments to be competitive. This scheme made Bitcoin network in good shape over time.

Bitcoin is deflated by design: That means BTC value is getting higher over time. Since mining is the only way to inject more BTC into the system so the amount of BTC in the system increase slowly that will keep BTC in high demand.

Bitcoin provides a scheme to keep BTC deflated over time by limiting the amount of BTC injected into the system.

The incentive BTC per a winning block will be decreased by halving every 4 years.

Starting at	50 BTC	in Jan 2009.
Halved to	25 BTC	in 2012.
	12.5 BTC	in 2016.
	6.25 BTC	in 2020.
	3.125 BTC.	April 19, 2024.

And will be halved again in 2028.

BTC Units: One BTC is sometime called a bit.

Centi BTC (cBTC) = 10^{-2} BTC, Milli BTC (mBTC) = 10^{-3} BTC, Micro BTC (uBTC) = 10^{-6} BTC

Currently the smallest transferable unit is: a Satoshi = 10^{-8} BTC

The first exchange rates for Bitcoin were published in October 2009:

1,300 BTC for 1 USD Check: https://blockchain.info/charts

The mining incentive will reach the minimum (1 satoshi) in 2137.
Then there will be no more BTC minted after the year 2140 and the total BTC in the system will be less than 20.9999999 million BTC.
Since there were some unknown amount of lost BTC e.g. sending to invalid addresses or losing private keys. The total BTC would be unexpected less. After 2140, miners will make profit only from the transaction fees (tips).