



SNS COLLEGE OF ENGINEERING

(Autonomous)



Bitcoin

- Released in 2008 by Satoshi Nakamoto.
- Focus on crypto-currencies and micro-payments
- Proof of Work Consensus



Bitcoin vs. bitcoins

Bitcoin is the system

bitcoins are the units

What is Bitcoin?

- A **peer-to-peer** internet currency that allows **decentralized** transfers of value between **individuals and businesses**.

Before Bitcoin

- DigiCash (1989): The 1st Electronic Cash System
 - David Chaum's company, featuring *ecash* (1983)
 - Ecash notes backed by fiat from bank
 - Relied on blind signatures
- The idea was published in 2009 by an pseudonymous person/group of people, named **Satoshi Nakamoto**.

Goal with Bitcoin was:

- To create a **trustless** system, using cryptography
- Solve double-spending problem of previous digital currencies

- Create digital assets that can be owned, with proof of ownership

Creating a currency from scratch

- Motivation
 - Distrust of financial institutions
 - Transaction costs
- Primary concerns
 - Transaction security
 - Double spends

Distrust of financial institutions

- Any noncash transaction requires a trusted third-party administrator—commonly a bank or financial service provider.
- The system forces participants to trust financial institutions that are not always trustworthy.

Transaction security

- Two levels of verification
 - Source is legitimate
 - Coins are legitimate
- Public/private key verification ensures the legitimacy

Double spends

- If the money is just digital codes, why not copy and paste to make more money?
 - Timestamps
 - Hashes
 - Block chain
- Timestamp
 - Each transaction is packaged and publically recorded in the order it was carried out.
- Hash

- The time-stamped group of transactions are given a unique algorithmically derived number

Bitcoin

- **Bitcoin** is the official first cryptocurrency that had been released in 2009. It is basically a digital currency and only exists electronically.
- Bitcoin is the first successful electronic cash system and coincidentally, the first instance of a successful Blockchain.
- Secure, trustless, borderless
- No bank needed to authorize/process transactions
- Transactions are stored on a **distributed ledger**

Bitcoin introduced the concept of **cryptocurrency**; decentralized digital money secured by cryptography, and used to create valuable digital assets that cannot be counterfeited.

Bitcoin transactions are authorized in a peer-to-peer network.

- Each node stores the history of the chain of blocks, containing validated transactions
- Counterfeiting is impossible because if one node's history is corrupted the others stay the same, and no central authority (i.e. bank) needs to confirm; this is called **decentralization**
- Unlike previous P2P network models, members of the Bitcoin network are incentivized to participate through **cryptocurrency**.
- Specifically, the incentive is for the people who mint (create) Bitcoin, called **miners**.

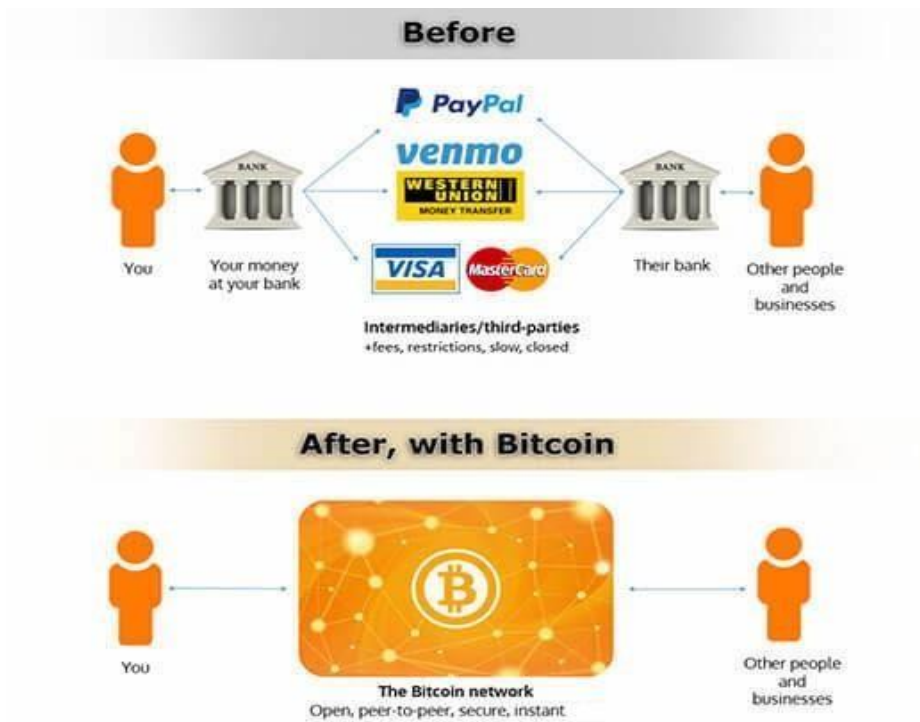


Figure 1.28 before and after bitcoin

Bitcoin Properties

- Bitcoins can be possessed.
- Bitcoins can be transferred.
- Bitcoins are impossible to copy.

Mining bitcoins

- Miners solve complicated algorithms to find a solution called a hash.
- Finding a hash creates a block that is used to process transactions.
- Each new block is added to the block chain.
- Until there are 21 million bitcoins, miners are paid for finding a hash in new coin.
- After 21 million, miners will charge transaction fees for creating a new block.
- The amount paid per hash goes down by half about every 4 years.

Owning bitcoins

- Users create accounts called wallets.
- Wallets are secured using passwords and contain the private keys used for

transferring bitcoins.



Spending bitcoins

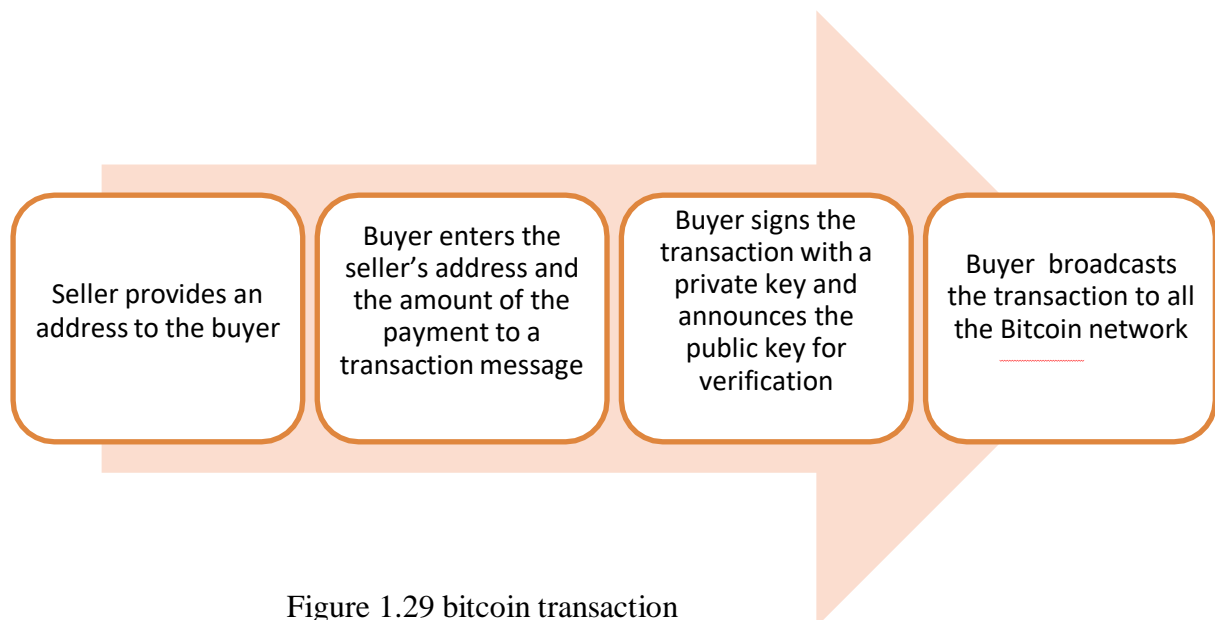


Figure 1.29 bitcoin transaction

Wallets

- A wallet is a combination of public address and private key.



Desktop wallets



Mobile wallets



Cold wallets/
Hot wallets



Online web wallets



Paper wallets



Hardware wallets



Bitcoin wallets

Figure 1.30 bitcoin wallets

Hardware wallets

- Most popular hardware wallets are Ledger Nano S and Trezor.



Figure 1.31 Hardware Walet

- Hardware wallets are hardware devices that individually handle public addresses and keys.
- It looks like a USB with OLED screen and side buttons.
- when you open a wallet (in the hardware wallet or software wallet) you are provided with 2 pair of keys (sometimes more).
- **Public key** and **the private key**.

- **public key** is used to generate the public **cryptocurrency address** you can use to receive the cryptocurrency,
- the **private key** is used to sign the transactions confirming your ownership over it.
- This is a reason why private key must be **kept secret**

Paper Wallets

- It is a physically printed QR coded form wallet.
- Some wallets allow downloading the code to generate new addresses offline.



Figure 1.32 Paper Wallet

Desktop Wallet

- Desktop wallets are programs that store and manage the private key for your Bitcoins on your computer's hard drive.





Electrum	Exodus	Bitcoin Core	Atomic Wallet
			
Type: SPV	Type: SPV	Type: Full node	Type: SPV
Beginner friendly: No	Beginner friendly: Yes	Beginner friendly: No	Beginner friendly: Yes
Platforms: Desktop only	Platforms: Desktop, mobile	Platforms: Desktop only	Platforms: Desktop, mobile
Visit website	Visit website	Visit website	Visit website

Figure 1.33 Desktop Wallet

Mobile wallets

- A mobile wallet is a virtual wallet that stores payment card information on a mobile device.
- They are quite convenient as it uses QR codes for transactions
- Some mobile wallets are Coinomi and Mycelium



Figure 1.34 Mobile Wallet

Web Wallets

- These wallets are accessed by internet browsers.
- They are the least secure wallets.
- They are not the same as hot wallets.
- They are ideal for small investments and allow quick transactions.
- Some of these are MetaMask and Coinbase.

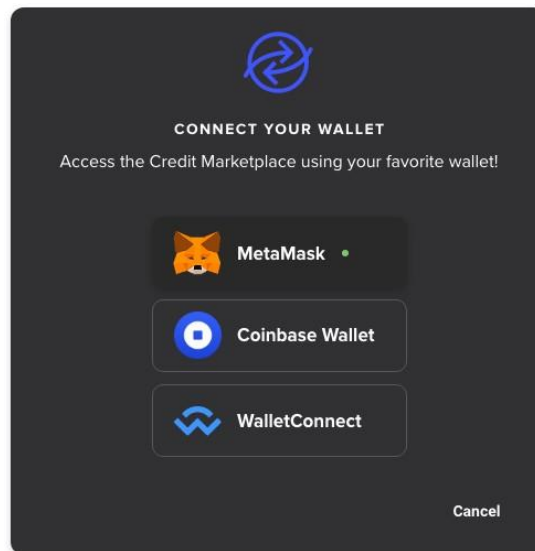


Figure 1.35 Web Wallet

Bitcoin Transactions

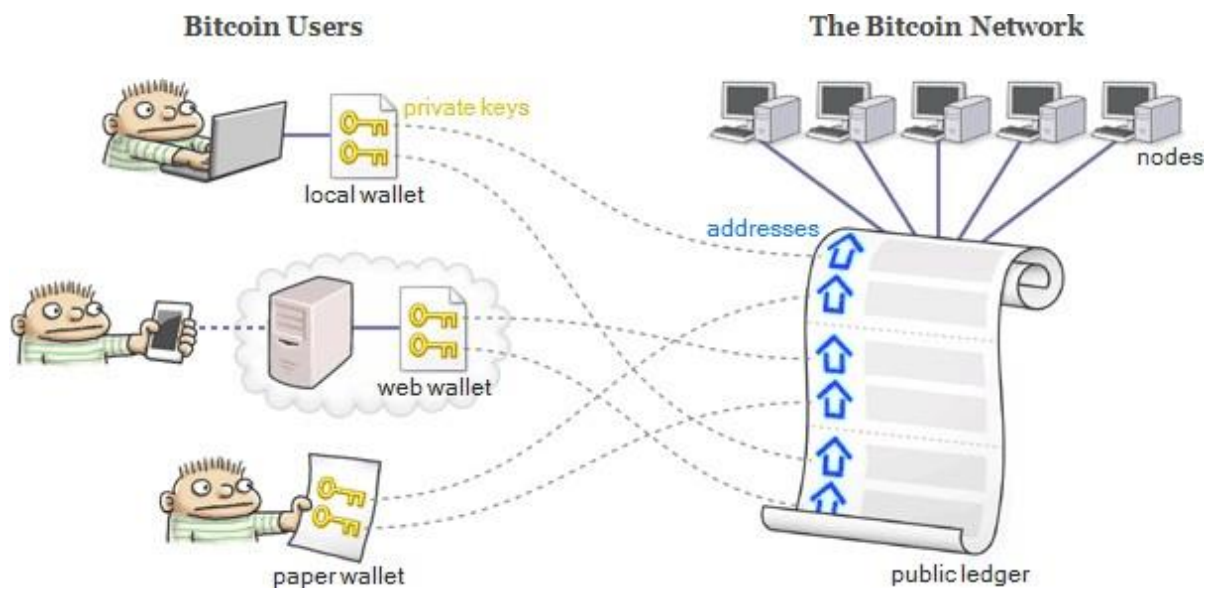


Figure 1.36 Bitcoin Transactions

- A full node is basically an electronic bookkeeper, and anybody in the world can set up and run one.
- Each node has a complete copy of the **public ledger** – that's a record of every Bitcoin transaction

Sample Transaction

		Debit	Credit
Transaction e14768c1d648b98a52cb796af30af186140c5209a2fb53f1c8097db579f01cc0			
INPUTS			
Previous Output	Signature		
6120ceaab25cfee257... : 0	3046022100aaf227f9...	0.0145	
6eb36c1d347f8fdb6e... : 1	3046022100810c9d7a...	0.0923	
OUTPUTS			
Address	Spent		
1NqUaJrFeStshjad1bhrEFFzWSQw6JHbqv	<input checked="" type="checkbox"/>		0.0122
1FrTrypBwstUQ4X9KQdQByx6fWXLGGuPNT	<input checked="" type="checkbox"/>		0.0945
Transaction b6f4ec453a021ac561b01039f78e7168a653af176353c86d607343cc77e779b9			
INPUTS			
Previous Output	Signature		
e14768c1d648b98a52... : 0	30450221008a396b69...	0.0122	
OUTPUTS			
Address	Spent		
1HiMoMgBaAikFHgAt3M4YJtetp4HrnsiXu	<input type="checkbox"/>		0.001
1Q3Jw1wRxZyJ767mVrTEpBVTH49HNBA83V	<input checked="" type="checkbox"/>		0.0111
Transaction ee7df4af6472ae93427824d39191ec5940282c4da8cad326a3eade81884fbc36			
INPUTS			
Previous Output	Signature		
b6f4ec453a021ac561... : 1	3045022100f112ff63...	0.0111	
OUTPUTS			
Address	Spent		
12MBAVJZ8pcVQQLMzHMWdxNvMFCxEgfk7P	<input type="checkbox"/>		0.001
1Muhz3LbdJsUS431aZbRwD1Cd5gLDQM8m8	<input type="checkbox"/>		0.01

Figure 1.37 Transactions with Hash values

- Every transaction has a set of inputs and a set of outputs.
- The **inputs** identify which bitcoins are being spent, and the **outputs** assign those bitcoins to their new owners.
- Each input is just a digitally signed reference to some output from a previous transaction.
- Once an output is spent by a subsequent input, no other transaction can spend that output again.
- Each unspent output represents some amount of bitcoin that is currently in someone's possession.
- Note that nobody's real name appears anywhere within a transaction. That's why Bitcoin

is often said to be **pseudonymous**.

- Instead of real names, bitcoins are assigned to **addresses** such as 1PreshX6QrHmsWbSs8pHpz6kLRcj9kdPy6.

Where Do Addresses Come From?

- Obviously, if you want to receive bitcoins, you need to have a Bitcoin address. Your wallet can generate addresses for you.
- In order to generate an address, your wallet first generates a **private key**. A private key is nothing but a large number roughly between 1 and 2^{256} .
- To make such numbers shorter to write, it's customary to [encode](#) them as sequence of numbers and letters.


5JrFqG1rMLy6SkoWcZktr3HGqTSaXj63VAvQJNrrj78Yhb1FtB 

Bitcoin Address

- Next, your wallet converts that private key to a Bitcoin address using a [well-known function](#). This function is very straightforward for a computer to perform.
- it uses elliptic curve cryptography to generate Bitcoin addresses
- If anyone knows your private key, they could easily convert it to a Bitcoin address, too.

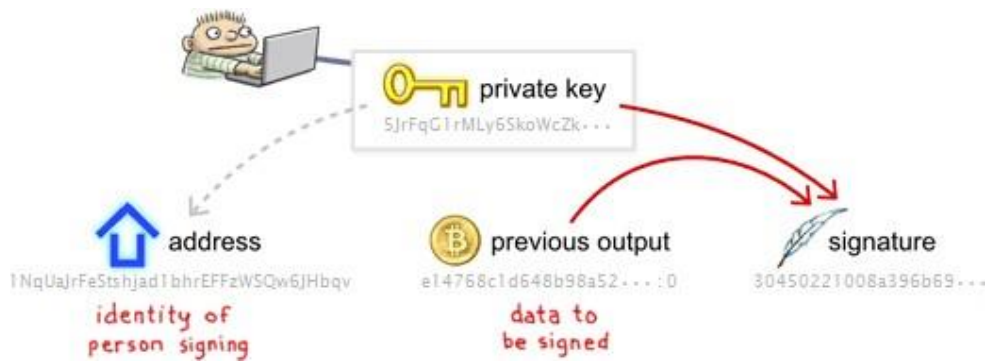
5JrFqG1rMLy6SkoWcZktr3HGqTSaXj63VAvQJNrrj78Yhb1FtB    1NqUajrFeStshjad1bhrEFFzWSQw6JHbqv

- If someone knows *only* your Bitcoin address, it's virtually impossible to figure out what the private key was.

   1NqUajrFeStshjad1bhrEFFzWSQw6JHbqv

How Are Transactions Authorized

- In Bitcoin, a valid digital signature serves as proof that the transaction was authorized by the address's owner.
- Just as a private key was required to generate that address, the same private key is required, once again, to generate a valid digital signature.



- A digital signature is only valid if a [specific equation](#) is satisfied by the address, the previous output and the signature.



The Bitcoin lifecycle

- Sender wants to send 1 Bitcoin to Receiver. This is what is going to happen:

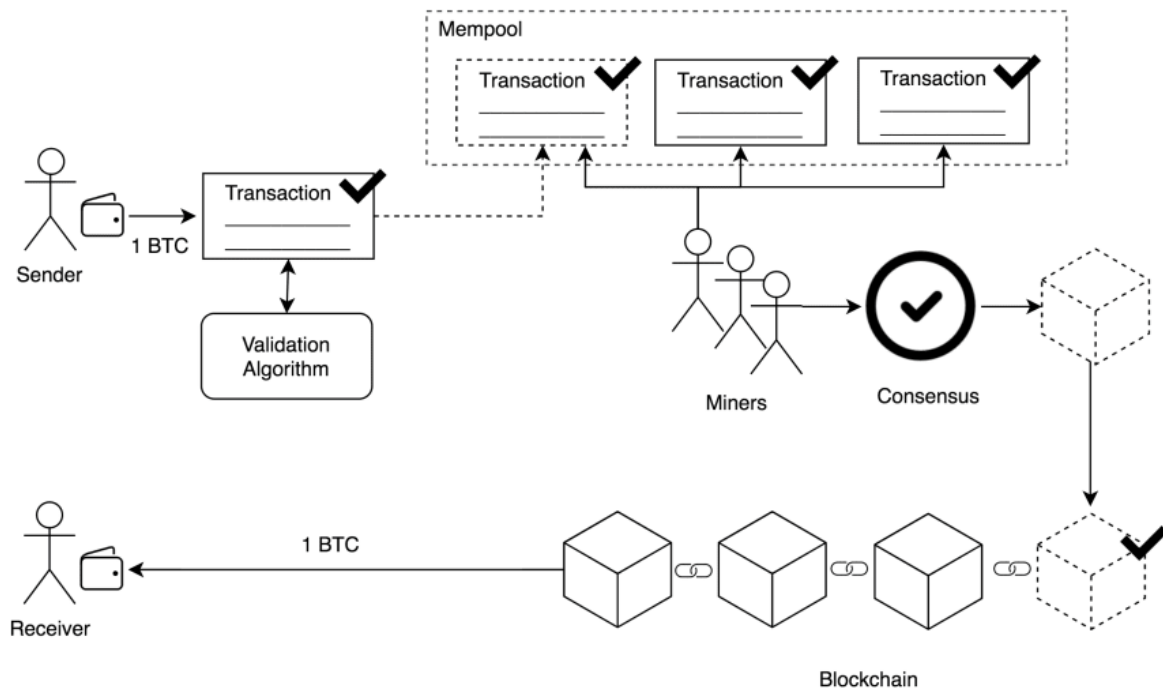


Figure 1.38 Bitcoin Life cycle

1. Sender creates a transaction.
2. Sender's bitcoin wallet validates the transaction.
3. The transaction is sent to Mempool.
4. Miners get the transaction from Mempool and start mining the block using a consensus algorithm.
5. After the block is fully mined, it is added to the network.
6. The chain validates the new block and every peer in the network will get the blockchain with the new block added.
7. Finally, the Receiver get your BTCs

Mempool

- The Mempool (Shortcut for Memory Pool) is where the transactions stay until the miner is ready to get them.
- In the bitcoin's blockchain, the miner prioritize the biggest transactions over the smallest ones.
- This happens because here is where the miner makes money.
- Miner "mine" the block through the consensus algorithm.

Bitcoin Flow of Transaction

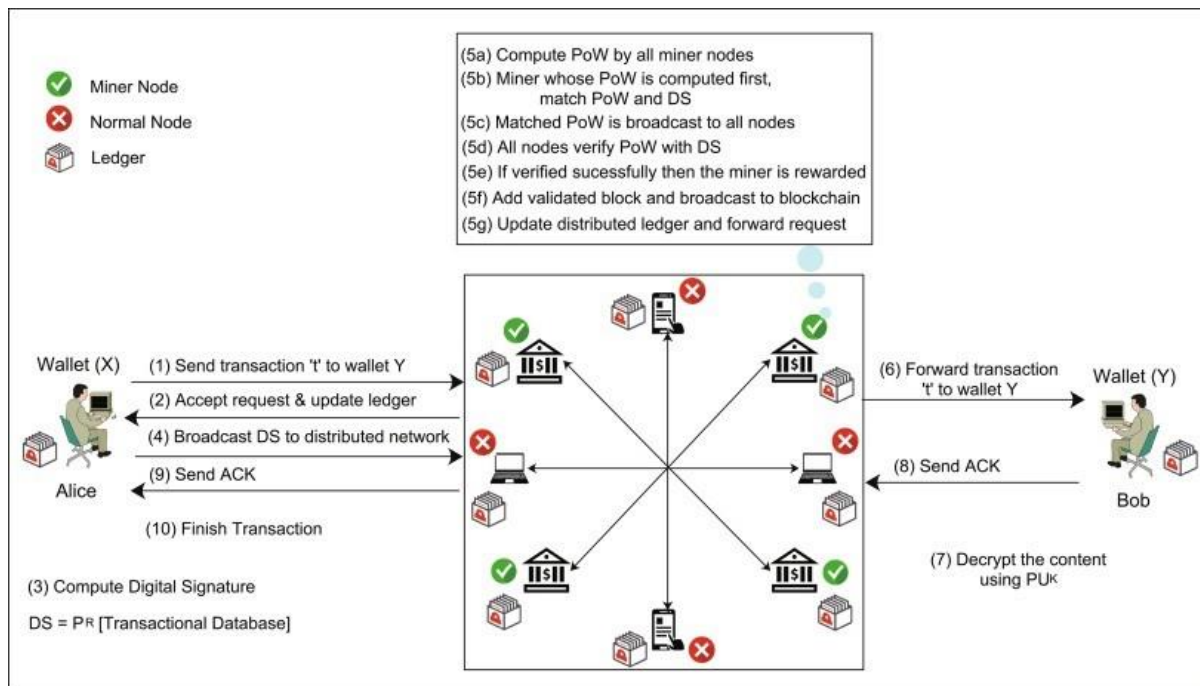


Figure 1.38 Bitcoin Flow diagram

- Let us say that there are two parties *Alice and Bob* who want to communicate with each other for funds transfer over an insecure channel, Internet. Then following sequence of activities are performed between two parties.
- If *Alice* wants to send some coins from her wallet *X* to *Bob's* wallet *Y*, then a request of transactional data "*t*" is sent to *Bob*. This request is broadcasted in the entire network.
- The distributed nodes accept the request and update their ledgers with the transactional information of *Alice–Bob*.
- After updating ledgers, *Alice* computes digital signature (*DS*) and broadcasts it in the network.
- A miner node is selected to verify and validate the transaction. It computes proof-of-work (PoW) to match the *DS* received. If PoW is successfully matched with *DS*, then the result is broadcast to all the nodes for verification and validation.
- The other miner nodes also verify the PoW with *DS*. If the verification is successful, then the miner node is (financially) rewarded for computing the PoW.
- The validated block is added in the validated chain and the transaction is broadcasted to the entire blockchain.
- Using the validated transaction "*t*," the bitcoins are added to wallet *Y* of *Bob*.
- *Bob* decrypts the content using the paired public key (*PUK*) of *Alice* and sends the acknowledgment (*ACK*) to *Alice*.
- The transaction is finished once *Alice* receives the transaction acknowledgment.

Consensus Algorithm

- The consensus algorithm is probably the most important part of any implementation of blockchain.
- The Bitcoin uses one consensus algorithm called Proof Of Work.
- Try to get the right nonce number by checking the hash created for the block until the result hash have the same number of zero's in it's prefix.
- This execution to try to get the right nonce number takes a lot of energy cost and

computational work, and that's why the miners get the fees from the transaction.

Proof of Work consensus algorithm

- Proof of Work” because it requires some type of work - usually computer processing.
- consensus algorithm is a set of rules that governs a blockchain network.
- It is an agreement on the rules of a specific blockchain and how users can participate in the network
- Miners who carry out the validation of transactions in the blockchain.
- Miners have downloaded the full Bitcoin blockchain and chosen to run it on powerful computers.
- These users ([nodes](#)) in the Bitcoin network are called “miners” because they check and prove the accuracy of a transaction in a process called [mining](#) - similar to the computation of a complex mathematical problem.
- Once a request to record and complete a transaction is disseminated into the blockchain, usually the [transactions with the highest fee](#) offered are selected to go into the next block on the blockchain.
- In order to reach consensus on a valid block in the blockchain, the Bitcoin algorithm provides a [difficulty](#) as a parameter that needs to be met for a block to be valid.
- This “difficulty” is regularly modified by the Bitcoin network depending on the computational power of the miners.
- Difficulty may be decreased or increased to maintain a constant speed at which new blocks are added.
- An arbitrary number called a nonce (the abbreviation for “number only used once”) is added to the block for purposes of cryptography.
- Miners alter the nonce until a value is found that gives the block's hash the required difficulty level
- Once this requirement is met the block cannot be changed without redoing the work.
- During hashing, an algorithm called a hash function is used to convert one value (the selected set of data) into a fixed-size as the output - the hash value, thus masking the

original value.

- A hash function cannot be reverse-engineered, meaning that the hash value cannot be used to find out the original data.
- Thus, the hash value is a “fingerprint” providing thorough authentication and ensuring that no tampering took place with the transmitted content.
- Each hash value contains information on all previous network transactions.
- The newly generated hash is checked against the current difficulty.
- A hash value always has to contain a specific number of zero-bits. If the hash meets the criteria of difficulty, it is broadcast to the other miners in the network.
- If it does not, another nonce is selected and hashed. Miners generate many hashes with different nonces until they find one that meets the needed criteria.
- This repetitive process is known as “mining” and now you know why it requires so much energy.
- Therefore, the first miner who finds a valid hash validates the block into a new block and gets a block reward in Bitcoin.

Disadvantages of Proof of Work

- Bitcoin transactions per second has been seven transactions,
- VISA network’s estimated 1,700
- vast amounts of energy are required for the mining process in the Bitcoin blockchain.
- larger mining pools have more computational power at their access and thus greater chances of mining valid blocks, putting individual miners at disadvantage.
- Source : <https://www.bitpanda.com/academy/en/lessons/consensus-algorithms-proof-of-work/>

Proof of Work Vs Proof of Stake

Proof of Work	Proof of Stake
Participating nodes are called miners	Participating nodes are called validators or forgers

Mining capacity depends on computational power	Validating capacity depends on the stake in the network
Mining produces new coins	No new coins are formed
Miners receive block rewards	Validators receive transaction fees
Massive energy consumption	Low to moderate energy consumption
Significantly prone to 51% attacks	51% attacks are virtually impossible

Proof of work and mining

- To create new digital currencies by rewarding miners for performing the previous task.
- **When you want to set a transaction this is what happens behind the scenes:**
- Transactions are bundled together into what we call a block;
- Miners verify that transactions within each block are legitimate;
- To do so, miners should solve a mathematical puzzle known as proof-of-work problem;
- A reward is given to the first miner who solves each blocks problem;
- Verified transactions are stored in the public blockchain.

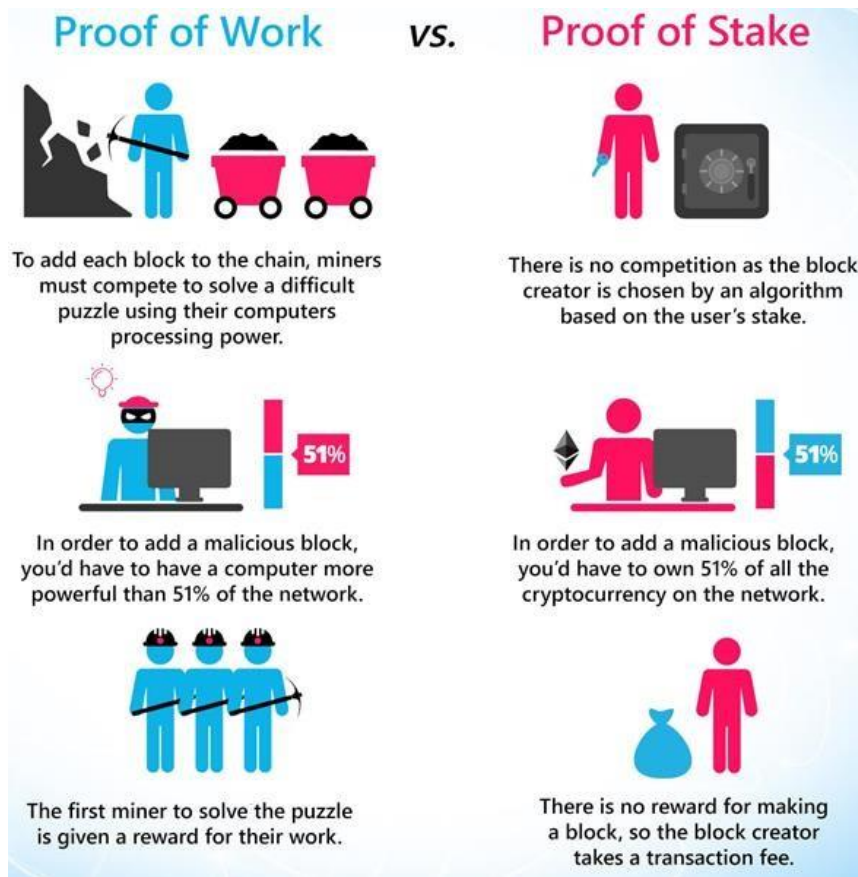


Figure 1.39 Proof of Work Vs Proof of stake

Mining Process

- From a technical point of view, the mining process is an operation of inverse hashing: it determines a number (nonce), so the [cryptographic hash algorithm](#) of block data results in less than a given threshold.
- This threshold, called difficulty, is what determines the competitive nature of mining: more computing power is added to the network, the higher this parameter increases, increasing also the average number of calculations needed to create a new block.

Bitcoin Address Example

- Bitcoin addresses are 26-35 characters long, consist of alphabetic and numeric characters, and either begin with “1”, “3”, or “bc1”.
- Currently, there are three Bitcoin address formats in use:

1. P2PKH (address starts with the number “1”)

- The P2PKH concept stands for “Pay to Public Key Hash”.

- P2PKH means “pay to this Bitcoin address”. It serves as an instruction on the blockchain for users wanting to transfer Bitcoin to one another.
- Behind every transaction, there are underlying codes working behind the scene. This scripting language is known as the Bitcoin Scripting Language.
- Example:

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2



P2PKH

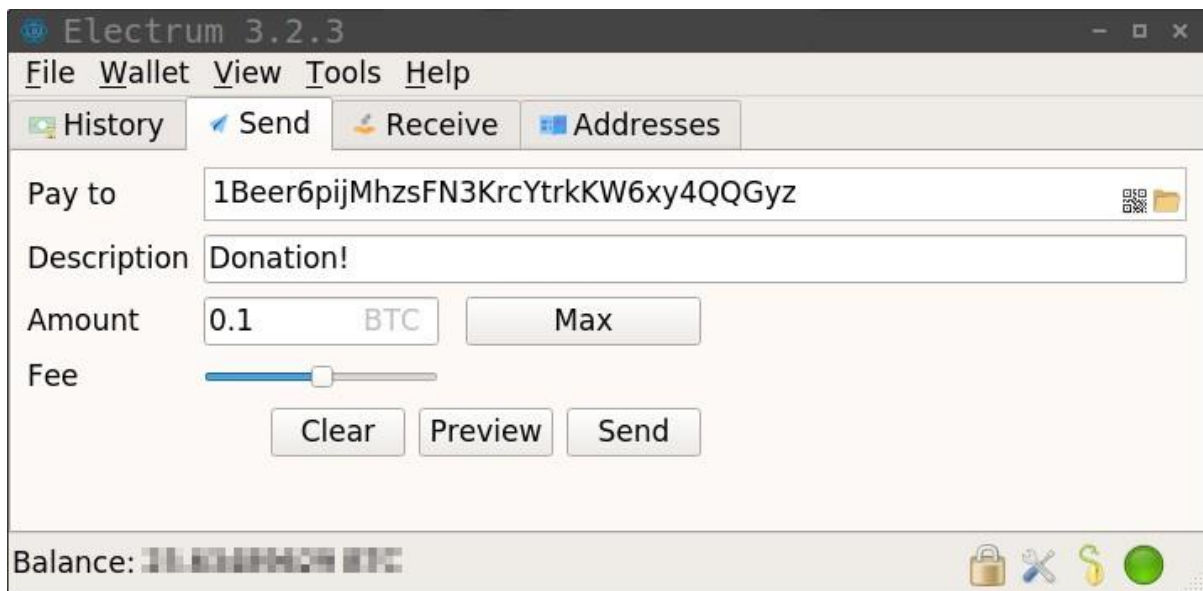


Figure 1.40 GUI of Pay to Public Key Hash

2. P2SH (address starts with the number “3”)

- Pay to script hash (**P2SH**) is an advanced type of transaction used in Bitcoin and other similar cryptocurrencies.
- P2SH or *Pay-to-Script-Hash* was a patch to Bitcoin added in 2012 which altered the way it validated transactions. It is most commonly identifiable as the addresses in Bitcoin that start with a “3” instead of a “1”.
- Unlike P2PKH, it allows sender to commit funds to a hash of an arbitrary valid script.

Example:

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

3. Bech32 (address starts with “bc1”)

Example:

bc1qar0srrr7xfkvy5l643lydnw9

re59gtzzwf5mdq

How to Get a Bitcoin Address

- To get a Bitcoin address, you first need to download a Bitcoin wallet, which is software that allows you to securely send, receive, and store Bitcoin funds in the Bitcoin network.
- Bitcoin wallets also store your private key, which is essentially your Bitcoin password.
- The software will generate a brand new Bitcoin address for you every time you create an invoice or receive a payment request for Bitcoins too.
- There are four types of Bitcoin wallets that you can use: [mobile, web, desktop, and hardware](#).
- Source: <https://blog.hubspot.com/marketing/bitcoin-address>