Introduction to Cryptocurrency Ecosystem

By Raj Thimmiah

How does a normal payment system work?

- Normal payment systems (generally) use ledgers
- Easy for servers to then check if someone is committing double spending

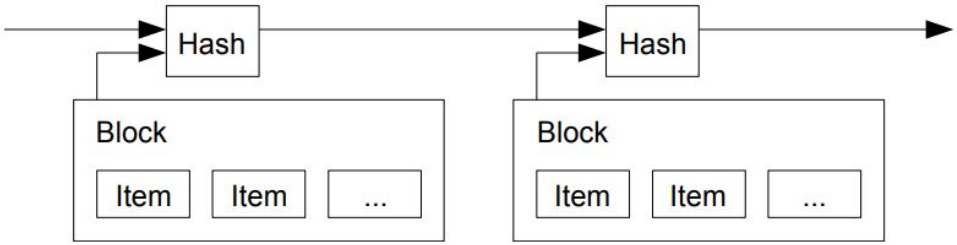
Account	A	B	C	D
Initial	75	60	10	100
Transfer	-50	+50		
Transfer		+15	+15	
Transfer	-25			+25
Transfer		-40	+40	
Transfer			+200	-200
Transfer	+50	-50		

Distributed Ledger Technology

- For a distributed system, there needs to be a way to ensure that all transactions are valid and people are not spending money they don’t have
- To do so, there must be a way to have a ledger that has transactions in an order that is agreed upon by all participants
- A timestamp server would do this but would require a central authority
- Instead, the **Blockchain** is used

Blockchain

- A Blockchain functions as a distributed ledger with all transactions divided into blocks that are newly created at roughly set intervals
- The order in which the blocks occur is the order in which the transactions occur allowing network participants to be able to check the validity of any transaction
- The blockchain is used in conjunction with **consensus algorithms** to decide upon the creation of new blocks and which transactions that the network agrees are valid



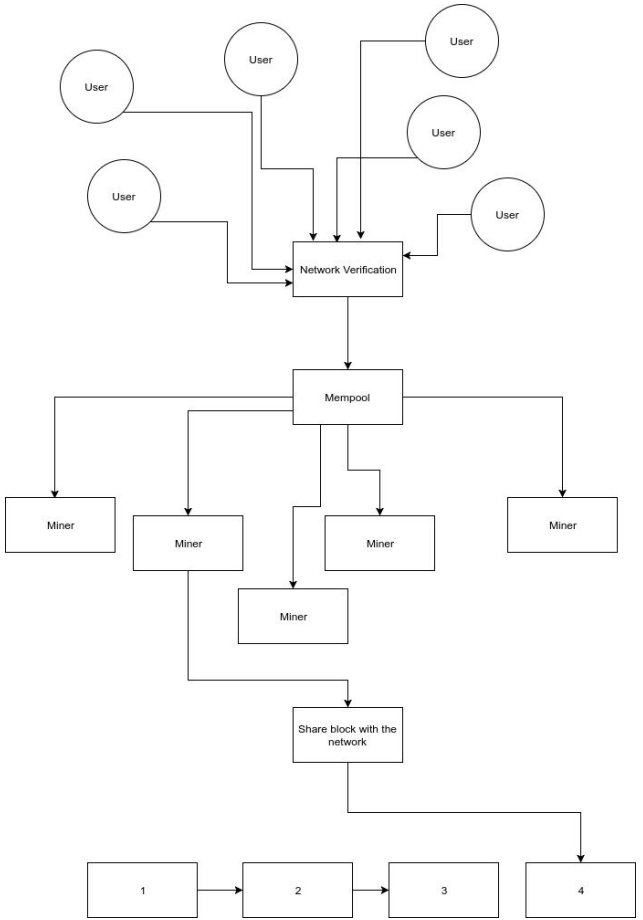
https://www.coindesk.com/short-guide-blockchain-consensus-protocols

Consensus Algorithms

- A consensus algorithm is used to do the following
  - Ensures that there is one agreed upon version of the blockchain
  - Prevents corrupt nodes from harming the network with fraudulent transactions or double spending (spending the same money in 2 places)
- **Proof-of-Work** is the most common consensus algorithm

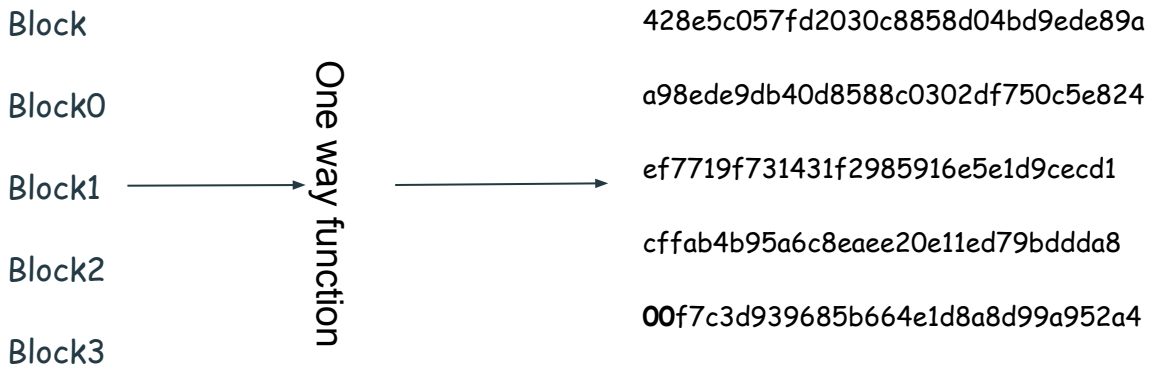
Proof of Work (PoW)

- Miners receive and pool transactions into blocks
- They attempt to solve a proof-of-work for these blocks that is computationally intensive
    - Blocks that are solved but not valid are rejected by the network
    - If successful and valid by network rules, the miners receive a reward



Proof-of-Work

- Proof of work involves attempting repeated hashes while incrementing a ‘nonce’ which is just an appended integer
- Once the output hash fulfills a specific criteria the block is considered to be solved

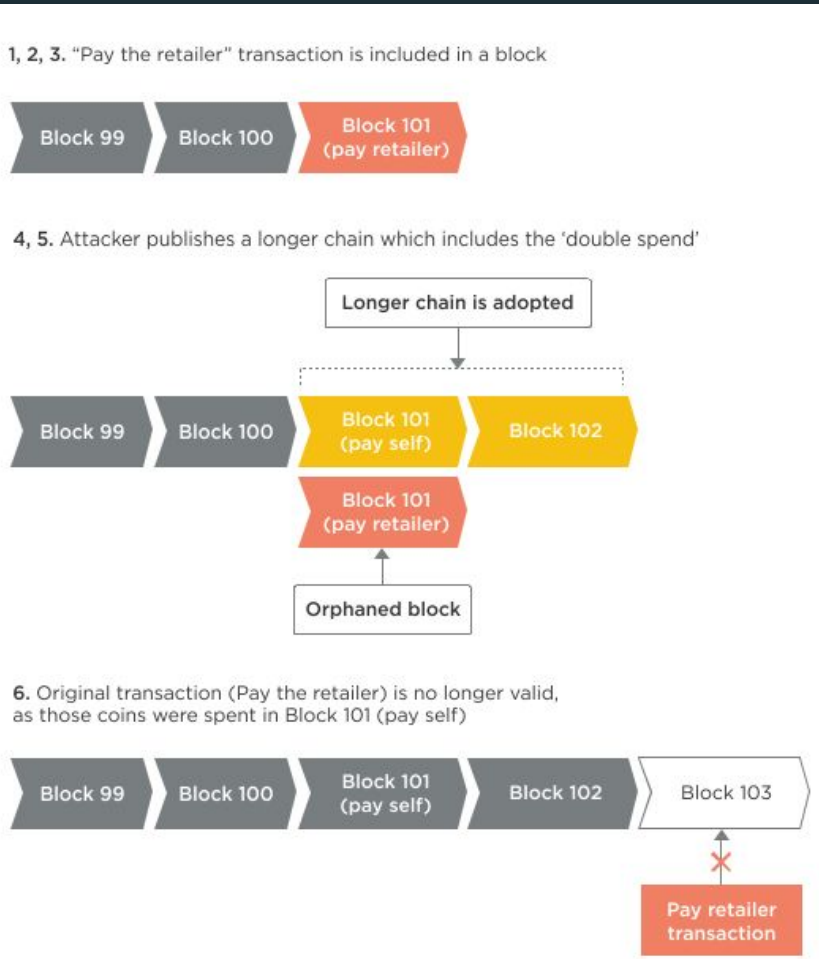


Tolerance

- If a corrupt miner pushes a block with faulty transactions, it will be rejected by the network
- The corrupt miner then has two options:
  - Push blocks with no transactions to slow down the network
    - A waste of money considering how profitable mining rewards are
  - To redo old blocks to **double spend**

Double Spending

- Has never been successful for Bitcoin
- Many merchants still wait for 6 confirmations regardless to minimize risk



Cryptocurrency Characteristics

- Blocktime
- Hashing algorithm/Consensus algorithm
- Transactions per second (Tps)

Economic

- Inflationary vs. Deflationary
- Max supply
- Premined
- Value/Use beyond speculation
- Fees (generally dynamic but can increase greatly if there is miner collusion/large backlogs)
- centralization of funds

Community

- Dev activeness/quality
- Development Centralization
- Level of community support/interest (“hodlers”)

Litecoin

Blocktime: 2.5 Minutes

Consensus algorithm: Proof of Work with Scrypt (memory intensive)

TPS: 28 tps, 56 tps post segwit

Supply: Max 84m, reward halved every 4 years

Fees: Avg. 0.089$

Litecoin vs. Bitcoin

Blocktime: 2.5 Minutes

Hashing algorithm: Proof of Work with scrypt

TPS: 28 tps, 56 tps post segwit

Supply: Max 84m, reward halved every 4 years

Fees: Avg. 0.089$

Blocktime: 10 Minutes

Hashing algorithm: Proof of Work with SHA256

TPS: 3.5-7 tps, 11+ tps post segwit

Supply: Max 21m, reward halved every 4 years

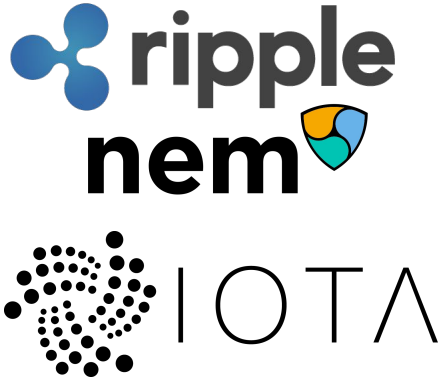
Fee: Avg. 6.24$

Currencies

Platforms:

Security/Privacy:

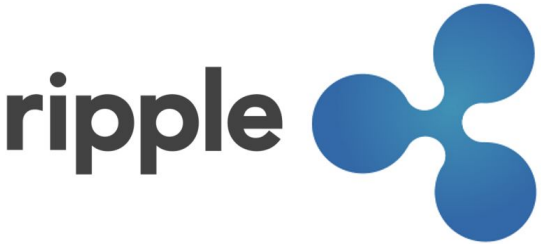
Application Specific:



Currencies

Security/Privacy:

Application Specific:



Blocktime: 3-4 seconds

Consensus algorithm: Ripple Protocol Consensus Algorithm (RPCA)

TPS: 1,000+

Dev team: a company also known as ripple are the primary developers behind XRP

Intent: To replace banking channels such as SWIFT and to enable faster global payments

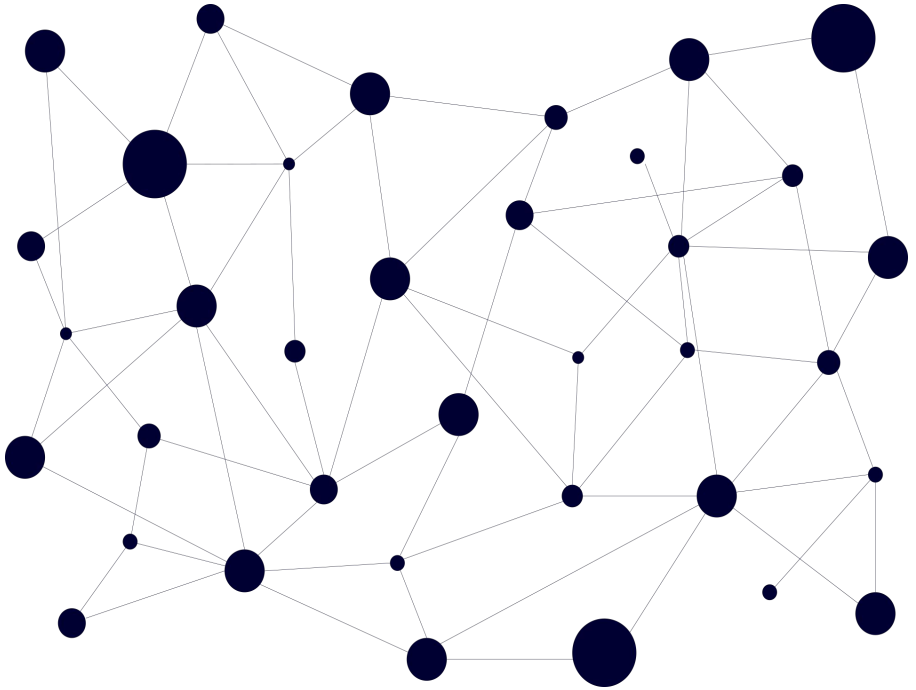
Fees: less than a cent

https://ripple.com/files/ripple_consensus_whitepaper.pdf

Ripple Protocol Consensus Algorithm

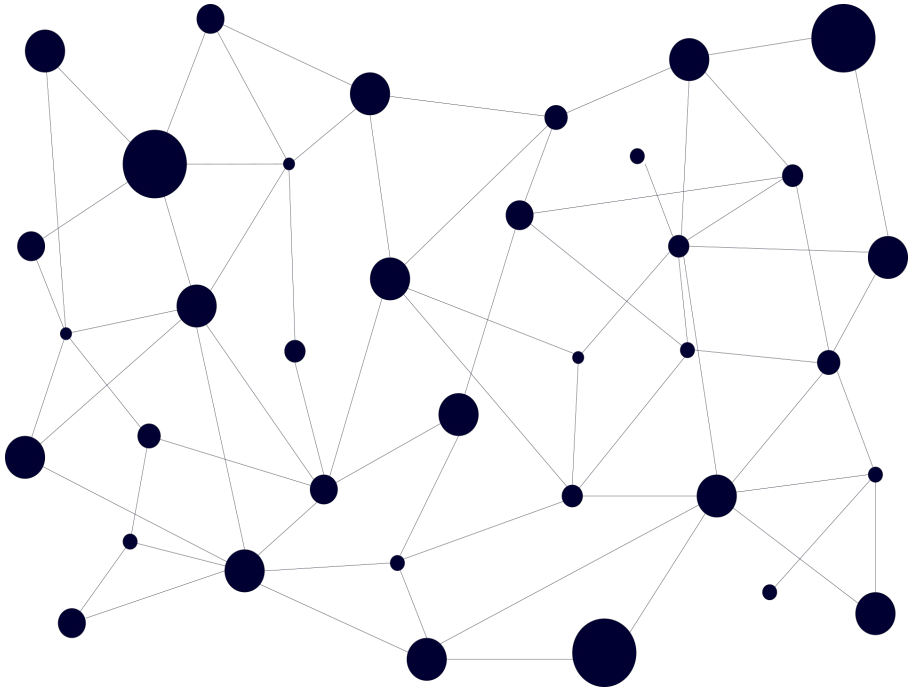
Each server node on the network has a Unique Node List (UNL) comprised of trusted nodes
proceed in rounds as such:

- Each server node creates a ‘candidate set’ of transactions that have not already been applied
- Each server gathers the candidate set of all the of the nodes on its UNL
- Nodes then vote on the veracity of transactions, requiring 80% ‘yes’ for them to be passed
- Thus, as long as at least 80% of nodes are honest the network is safe
- There can also be multiple rounds of voting on transactions



Ripple Protocol Consensus Algorithm

- What prevents nodes from stalling and withholding votes to slow down the network?
  - Nodes that have a higher latency than threshold *b* are dropped from the UNL list of other nodes
- What is the threshold for faulty nodes?
  - weak correctness (will only fail all transactions) can survive with up to 20% being faulty nodes and voting no for everything (though such nodes are eventually dropped)
  - strong correctness (will pass faulty faulty transactions) can survive up to 80% faulty nodes



RPCA Centralization

- By having a UNL that specifies which nodes are actually considered, it prevents Sybil attacks
- The UNL list is chosen by Ripple (the company) such that it is composed of banks, exchanges, and other partners that it trusts
- This makes the network still distributed while also being centralized

https://bitcoin.stackexchange.com/questions/50922/whats-a-sybil-attack

Ripple

Advantages:

- Extremely fast
- Highly scalable
- Low fees
- Strong partnerships with banks
- Solid devs

Disadvantages:

- not entirely centralized but the UNL list still causes a strong degree of centralization
- The Ripple company has a large number of the XRP token (though the majority is locked and only around 1 billion xrp is available to them per month)
- Devs are also centralized

Blocktime: 1 Minute

Consensus algorithm: Proof of Importance

TPS: 10 tx/s, will increase with the launch of Catapult which will convert the codebase from Java to C++

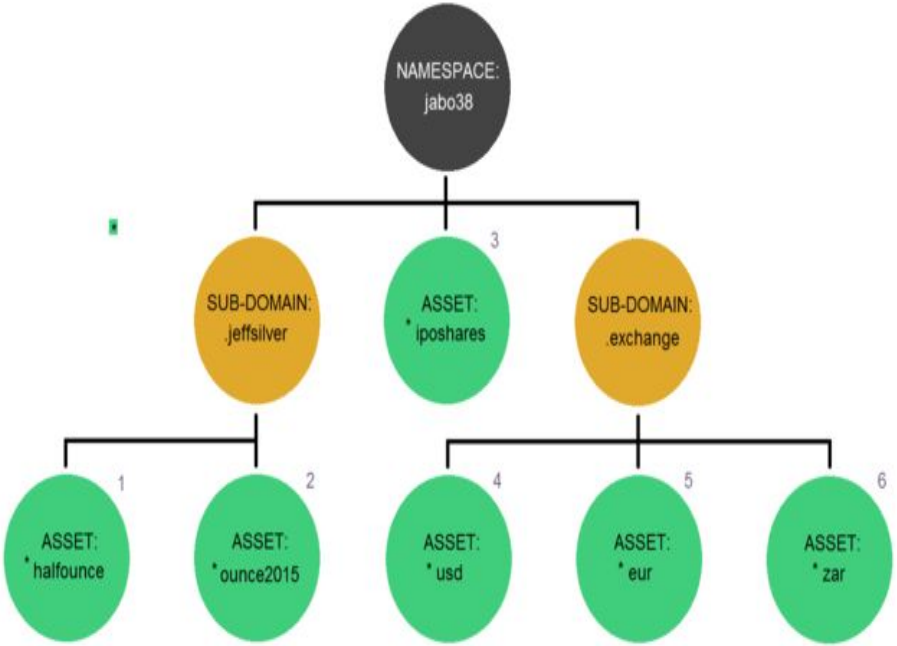
Dev team: Anonymous devs and some public figures

Transaction Fees: less than 20 cents

Note: token for NEM is referred to as XEM

Namespaces

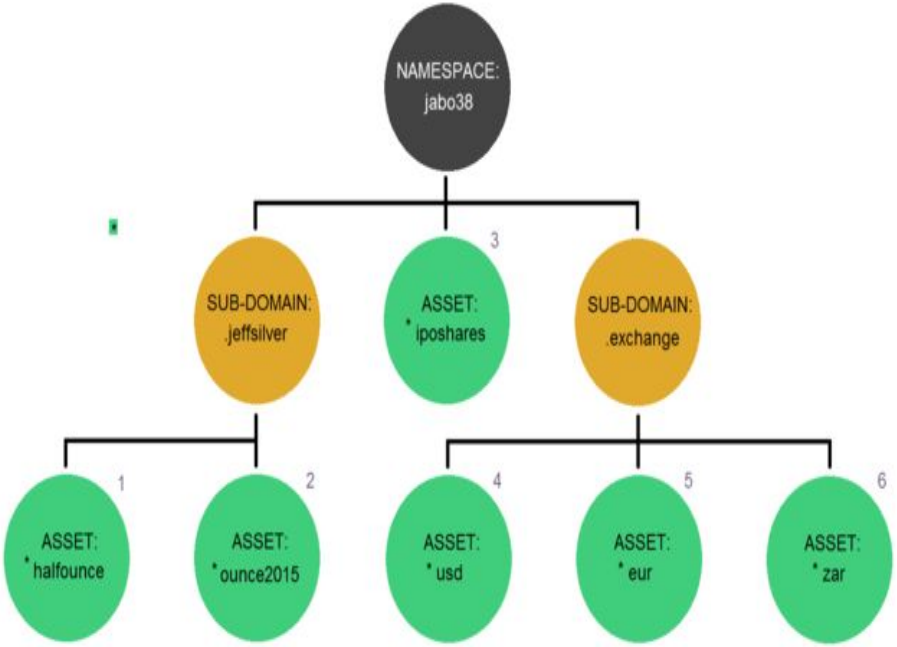
- Namespaces are similar to domains
- Only the root namespace needs to be unique, the sub-domains can be anything
- The intended usage of namespaces is to allow for categorizing '**mosaics**'



https://blog.nem.io/maing-namespaces-and-mosaics/

Mosaics

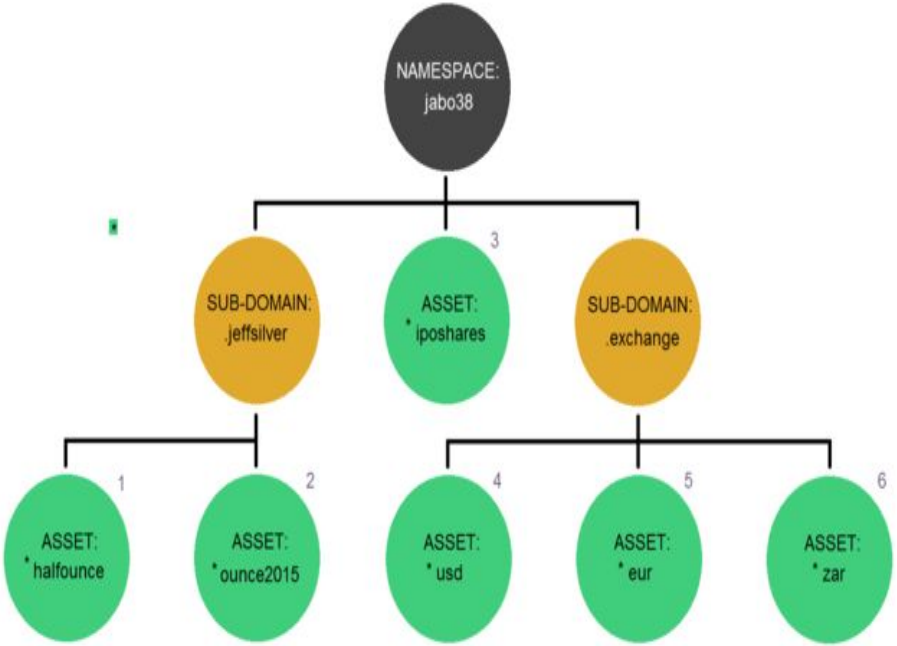
- Mosaics are digital assets that can have the following characteristics:
  - Initial supply (the amount of the asset that is created to start)
  - Divisibility (how many decimal places can be used)
  - Transferable (can be sent between people or only between people and original creator)
  - Mutable (supply can be created or deleted)



https://blog.nem.io/maing-namespaces-and-mosaics/

Mosaics

- In the case of the example on the right, halfounce would be
  - Jabo38.jeffsilver:**halfounce**
  - I could also create raj.jeffsilver:**halfounce** if I wanted to without issue
- If I was selling t-shirts, and wanted to represent one that had been sold
  - I could create raj.shop:t-shirt and permit myself to create as many as I want to represent new t-shirts
  - I could send one t-shirt token to every person to buy a shirt from me



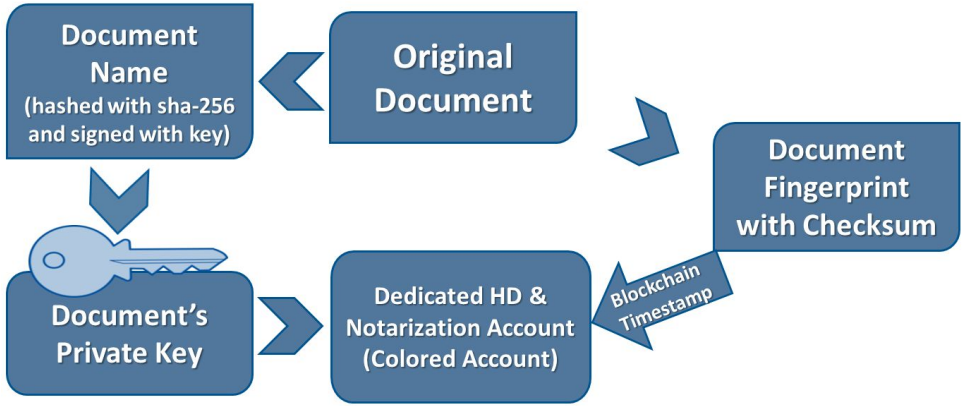
https://blog.nem.io/maing-namespaces-and-mosaics/

Multisignature/Multiuser accounts

- Multisig accounts let multiple users (parents) have control over a ‘child’ account
- In order to send any kind of transaction or initiate an action on behalf of the child account, x of n parents must agree
- Maximum of 32 ‘parents’
- In contrast to most other cryptocurrencies, this is done using built-in functions, not wallet dependent

Apostille

- Apostille is a built-in blockchain notary
  - Notaries prove the authenticity of a document as well as proving that it existed at a time
- With notarization, an account is created for the file which is owned by the one who is notarizing the document
- With private notarizations, files can be updated and be shown in a transparent manner
- Notarization accounts can be transferred or have their ownership split with other users
- Can also be marked with a namespace that you own



https://blog.nem.io/apostille-tutorial/

Proof of Stake Consensus Algorithm

- For most cryptocurrencies, any node can join and if individual nodes receive power for just existing a ‘sybil’ attack is a strong risk
- Thus, many cryptocurrencies weight nodes by the amount of the currency that they store
- A random node is then chosen (similar to a lottery ticket) wherein the more of the currency you have, the higher the chance that you are the one who creates the next block and get the rewards
- This does not reward nodes that help the network as full nodes nor does it take into account how long those coins have been held
- It makes a 51% attack (where the stakers could then prevent transactions) hard because you would need to control 51% of the entire supply

https://www.investopedia.com/terms/p/proof-stake-pos.asp

Proof of Importance

- Uses a reputation system that allows
  - Nodes to see which other nodes they should connect to
  - Allows for the creation of new blocks
- Similar random lottery as in proof of stake, but beyond just stake the following characteristics are considered:
  - Vested amount of XEM (amount vested is based on how long it has been in your account)
  - EigenTrust reputation based on transactions to and from the account
    - Prevents inactive accounts that are only harvesting from being able to reap all the rewards
- In nem, the successful ‘harvester’ receives all the transaction fees of that block
- Thus, the more transactions the network has, the better it is

https://www.youtube.com/watch?time_continue=1001&v=AiXFamTZWzk

Nem

Advantages:

- While not a general purpose platform, it still excels in many ways for the features it does implement
- Has strong enterprise support in Japan
- By prioritizing those who help the network, it has a higher chance of more people maintaining full nodes

Disadvantages:

- Intentionally does not have smart contracts
- Strong dev centralization with fees for many actions going to the devs as opposed to the network

Blocktime: 2.5 Minutes

Consensus algorithm: Proof of Work with X11 and Proof of Service

TPS: 28, can scale to 1500+ after Evolution upgrade

Dev team: Dash foundation, some level of governance by the community

Transaction Fees: 3-20 cents

Intent: Anonymity, governance, instant transactions

Full Nodes

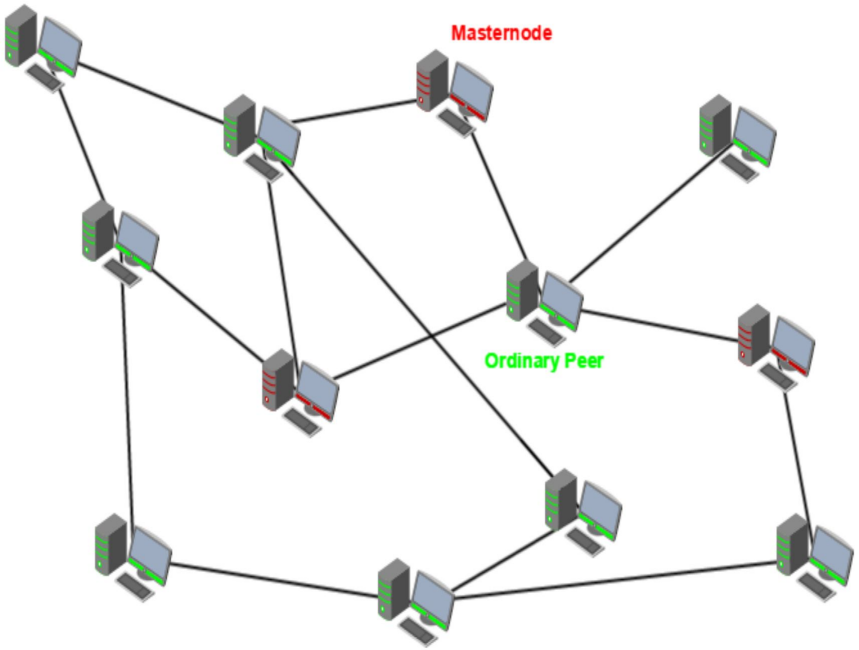
- Map of all Bitcoin full nodes
- Network depends on these full nodes for
  - Block and transaction propagation
  - Checking validity
- No incentive for most cryptocurrencies

Proof of Service

- Dash utilizes a variation of Proof of Stake that is often referred to as Proof of Service
- In many other cryptocurrencies there is a need for full nodes to propagate transactions, verify them as well as blocks for validity, and to spread copies of the entire blockchain to new nodes
- Over time as the size of the chain increases, less and less people operate full nodes due to the amount of storage and bandwidth required
- Dash's Proof of Service was created to counter that and to provide an incentive for people to offer services to the network in the form of "masternodes"

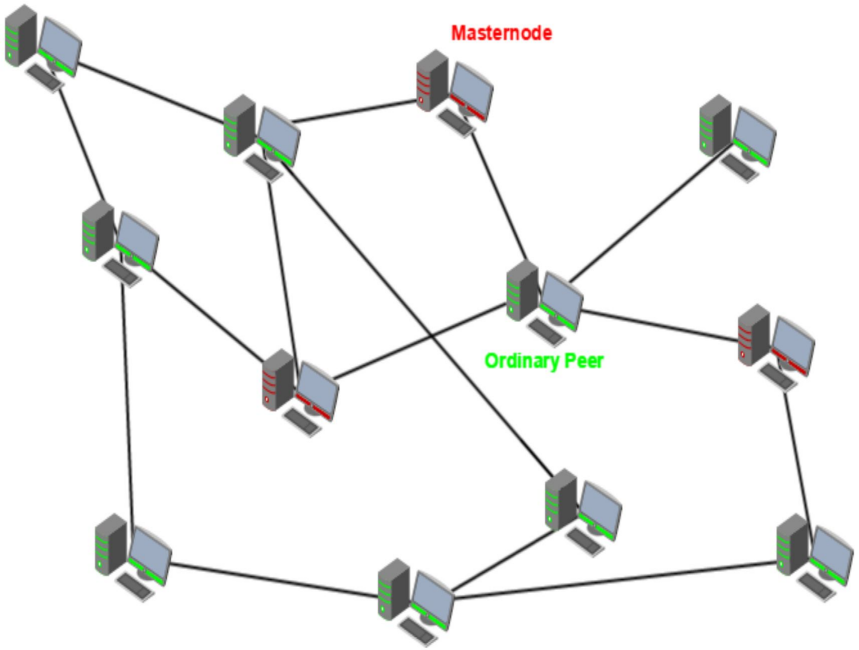
Masternode Network

- To host a masternode, you must put up 1,000 Dash which you cannot use while operating the masternode
- Masternodes perform various services for anonymity as well as other features
- To prove that the masternodes are actually doing work, masternodes are scheduled to ping other random masternodes to ensure **proof of service**
- Masternodes are rewarded by a percentage of the normal proof-of-work block reward
- With the current number of masternodes, they each receive an average of 2 dash per week
- [Masternode Network]



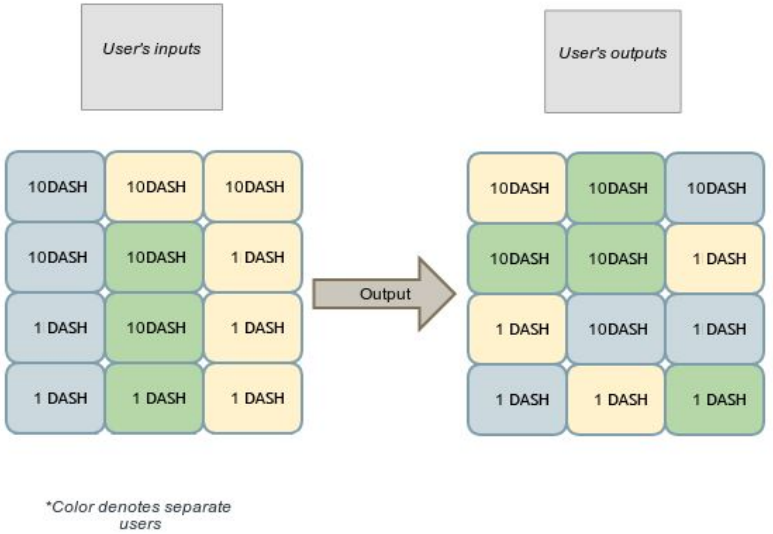
Masternode Network

- Requires stake of 1,000 Dash (300,000$)
- Perform services for the network
- To verify work, masternodes randomly ping each other (Proof of Service)
- Rewarded with a portion of the standard PoW block reward
- With the current number of masternodes, they each receive an average of 2 dash per week
- Stability to price
- [Masternode Network]



PrivateSend

- In most cryptocurrencies, if you send money to an exchange or someone who knows your identity, your previous transactions can be de-anonymized
- PrivateSend uses a mixer involving masternodes to anonymize user funds
- The more rounds of anonymization you go through, the harder it is for an adversary to recover your identity



InstantSend

https://www.reddit.com/r/dashpay/comments/5wv9it/how_does_instandsend_technically_work/

https://dashpay.atlassian.net/wiki/spaces/DOC/pages/58523665/Quorum+Selection

InstantSend

- Allows merchants to receive Dash in just seconds
- User sends a transaction with a flag that shows that they want to use InstantSend
- A set of 10 randomly selected masternodes (referred to as a quorum) then vote on the transaction
- If they find it to be valid, they then agree to lock up the funds and tell the rest of the network
- This prevents users from attempting to spend again as if they do the same set of nodes will check and know that it is invalid

https://www.reddit.com/r/dashpay/comments/5wv9it/how_does_instandsend_technically_work/ https://dashpay.atlassian.net/wiki/spaces/DOC/pages/58523665/Quorum+Selection

Decentralized Governance by Blockchain (DGBB)

- DGBB is meant to assist community efforts and projects
- Decentralized funding
- Users can submit proposals to the network
- Each masternode operator receives one vote for each proposal
- For a proposal to be passed, the following formula is used
  - (YES VOTES – NO VOTES)> (TOTAL NUMBER OF MASTERNODES * 0.1)
- If the number of passed proposals goes over the budget for the month, then the proposals are payed out in order of number of votes
- Dash proposals

https://dashpay.atlassian.net/wiki/spaces/DOC/pages/19169430/Using+Decentralized+Governance+Proposals+Voting+and+Budgets

Decentralized Governance by Blockchain (DGBB)

- A portion of the block reward (10%) is set aside each month
- Users can submit proposals to the network which are then voted on by the network once a month
- Each masternode operator receives one vote for each proposal
- For a proposal to be passed, the following formula is used
    - (YES VOTES – NO VOTES)> (TOTAL NUMBER OF MASTERNODES * 0.1)
- If the number of passed proposals goes over the budget for the month, then the proposals are payed out in order of number of votes
- Dash proposals

https://dashpay.atlassian.net/wiki/spaces/DOC/pages/19169430/Using+Decentralized+Governance+Proposals+Voting+and+Budgets

Dash

Advantages:

- Useful governance system
- Does not depend overly on centralized devs as funding can be re-allocated
- Introduces a fair level of privacy with PrivateSend
- Stable as most of the supply is staked in masternodes

Disadvantages:

- PrivateSend can be attacked if an adversary wants to enough and has upwards of 100,000,000$
- Proposals depend on the masternodes voting in the interest of the community

Monero

Blocktime: 2 Minute

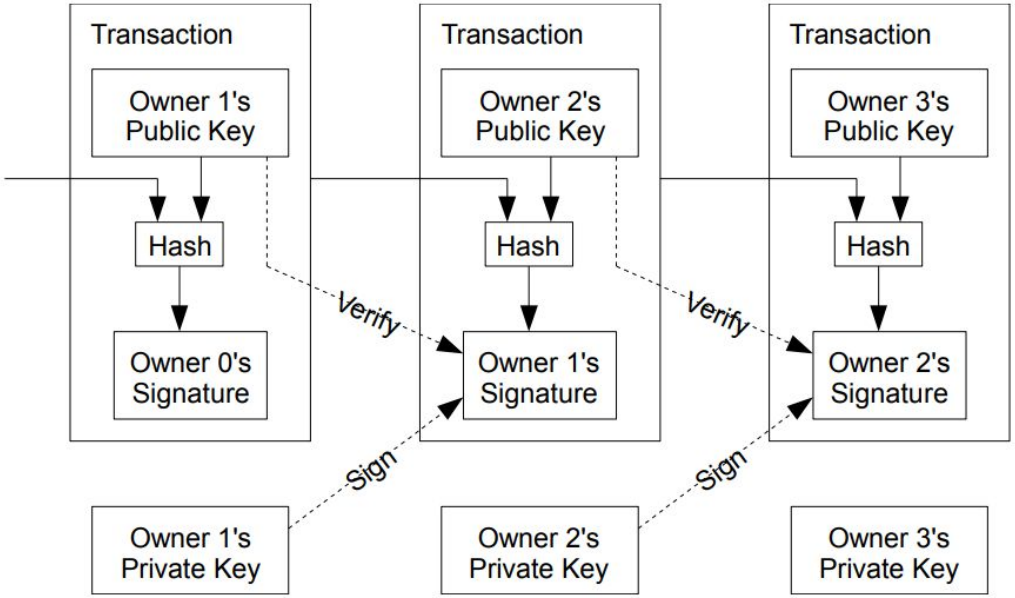
Consensus algorithm: Proof of Work with CryptoNight

TPS: 1500+, constrained by bandwidth and memory

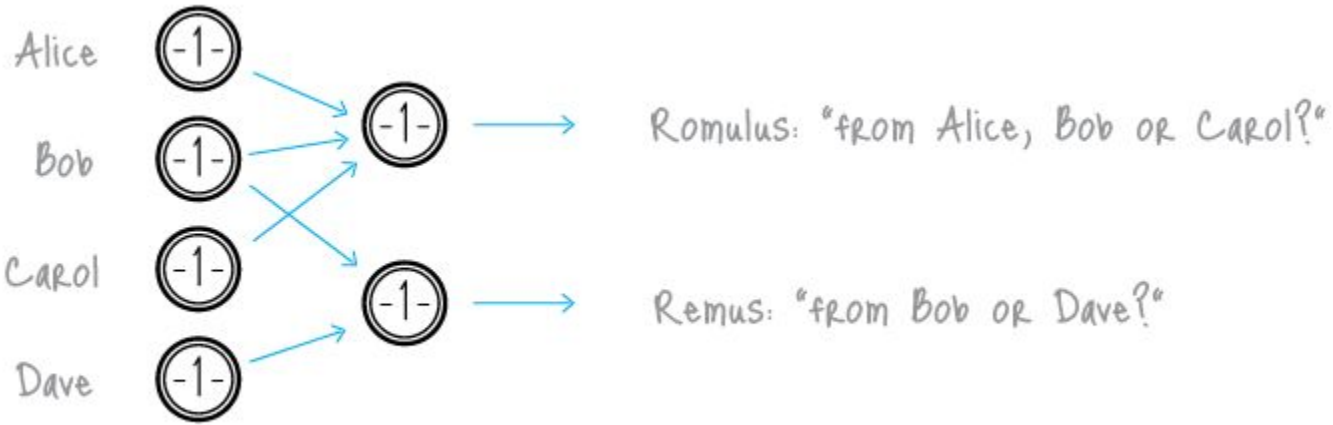
Transaction Fees: .35-1.5$

Intent: Anonymity

Standard Transactions



Ring Signatures



https://people.csail.mit.edu/rivest/pubs/RST01.pdf

Ring Signatures

- By using ring signatures, it becomes impossible to tell who the actual sender was as it could have been any of them
- In the wallet, other random public addresses are used on sending a transaction
- This will also result in your own public address being used randomly which can lead to it appearing as if you have made hundreds of transactions which no one can confirm are yours or not
- Effectively makes it extremely difficult to find who the sender is

https://people.csail.mit.edu/rivest/pubs/RST01.pdf

Unlinkable One Time Addresses

- Instead of sending to normal addresses, as is common with most cryptocurrencies, a one time address is generated using the receiver's public key + random data from the sender
- The only person who can know who the receiver is would be the reciever themselves who can check if a transaction belongs to them with a private view key (which they can share with others if they wish to reveal what they have received)
- Thus, every wallet user must check all transactions to see if they were intended for themselves or not
- Diffie-Hellman Exchange

https://www.monero.how/how-does-monero-work-details-in-plain-english

Preventing Double Spending

- With no link between senders and receivers, it is impossible to check for double spending since you can’t check if the person actually has the funds
- A key ‘image’ is used in order to prevent double spending while also allowing everyone involved to remain anonymous
- For every transaction, a key ‘image’ is generated from the sender’s public key one time address and their private key
- If the key image is ever used again the transaction will be flagged as double spending
- Thus, each one time address can be used only once
- If you don’t want to send the entire balance to another user, you send the remainder back to another address that you own

Other Cool Monero Features

- RingCT
  - Implemented January 2017, it also hides the amount that is being sent
- I2P Kovri Implementation
  - Makes IP addresses on the network untraceable in order to further increase anonymity
- Dynamic mining difficulty, block sizes, rewards, etc.
  - All balanced in order to prevent many of the issues faced by other cryptocurrencies that use hard coded values
- Built in multi-signature support

Monero

Advantages:

- Has stronger privacy technology than the majority of cryptocurrencies
- Dynamic variables for what is generally hard coded in other cryptocurrencies
- Strong attention to privacy beyond just the cryptocurrency itself (I2P)

Disadvantages:

- Imperfect implementation with multiple attack vectors that have been exploited in the past
- Depends solely on CryptoNote, the company that created it
- **Not Quantum resistant, can be de-anonimized with quantum attacks**