FTEC 5520 – Week 5

Agenda – Blockchain technology – Week 6

1. Application of Cryptography to Blockchain
2. Recap of Bitcoin transactions and actions
3. Types of Blockchain: Public vs Private, Permissioned vs Permissionless
4. Proof of Work and Proof of Stake
5. Byzantine General's Problem
6. Miscellaneous about Bitcoins

Blockchain affecting business model

Blockchain is a type of distributed ledger in which value-exchange transactions (in cryptocurrencies like bitcoins or other tokens) are sequentially grouped into blocks that are cryptographically chained to previous blocks.

What is Blockchain?

Data Structure

- a blockchain refers to a series of blocks, which consists of a block header and a list of transactions, in chronological order

Distributed and decentralized network

- A blockchain network is a distributed and decentralized network where every network node synchronizes among others to stores the same blockchain data structure and executes the same transactions in the same order

Distributed Ledger

- every network node will eventually have the exact same copy of blocks.

Open and Transparent

- everyone can join a blockchain network or quit from it at any time

Pseudonymity

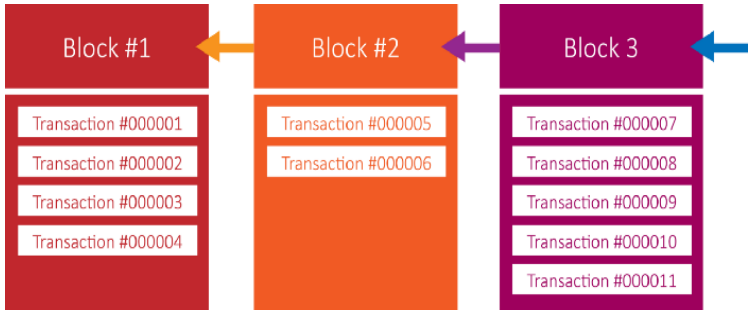
- Not required to disclose their real name
- All processed through address

Transactions are signed

- every transaction needs to be digitally signed by the originator to prove its authenticity.

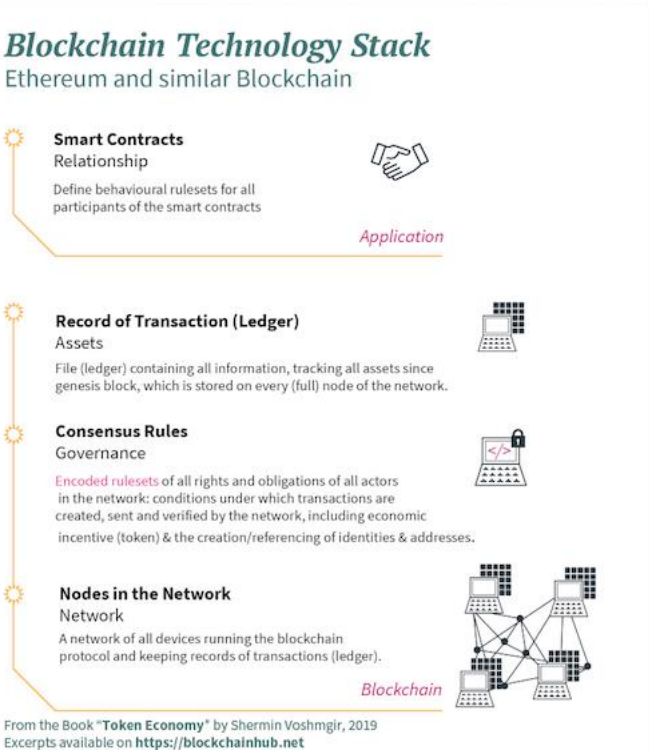
Immutable

- Once a transaction is being executed or stored, practically, no one can alter or delete the data, or undo the operation
- cryptographically secure transactional singleton machine with shared-state



Blockchain Technology Stack

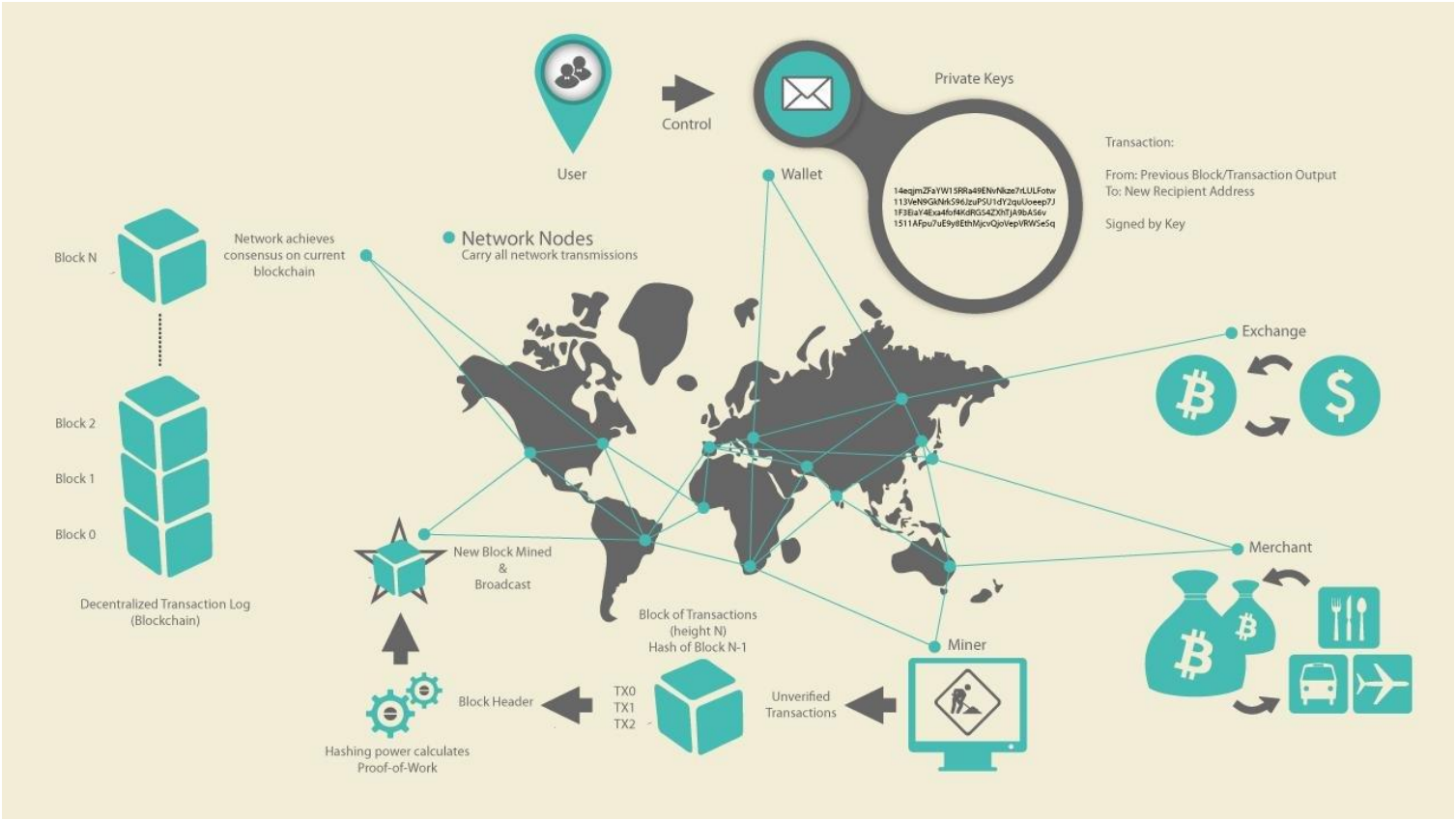
Elements / Components	Stack from the book
Data Structure used in the distributed ledger	Blockchain - Assets
Types of blockchain / DLT	Blockchain - Network
Consensus protocol	Blockchain - Governance
Token used / maintained	
Programming / Smart contract	Application - Relationship
Functionality of the blockchain / DLT	



Blockchain Technology Stack

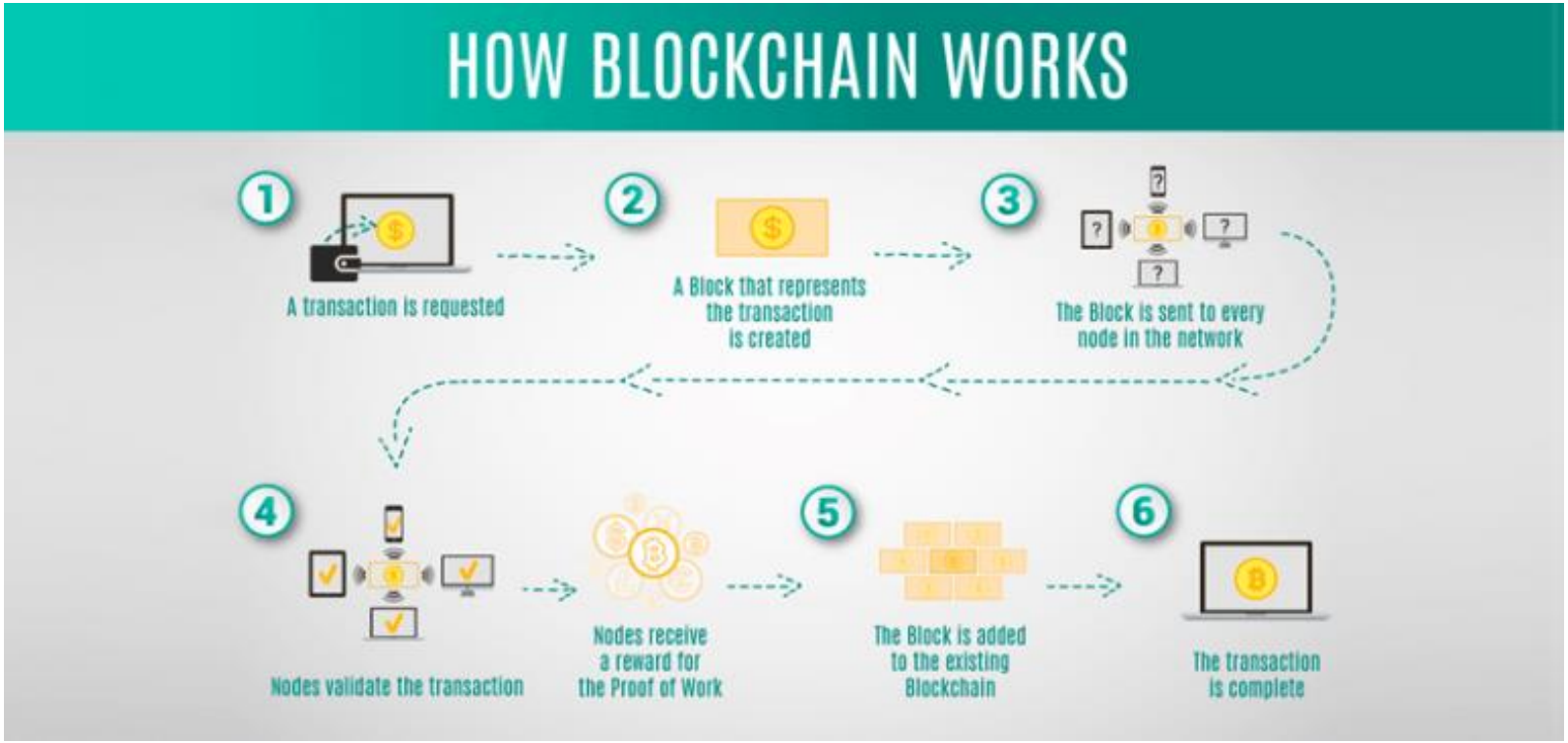
Elements / Components	Descriptions
Data Structure used in the distributed ledger	How data is being stored? How to ensure the immutability of the data? How to speed up verification of recorded data authenticity?
Types of blockchain / DLT	Is that public, permissioned or consortium type blockchain?
Consensus protocol	What kind of consensus protocol is used
Token used / maintained	Any token, cyber tokens, coins being used
Programming / Smart contract	Any implementation of smart contract
Functionality of the blockchain / DLT	Generic, specific type of blockchain?

Bitcoin overview (Recap)



From “Mastering Bitcoin”

How blockchain works

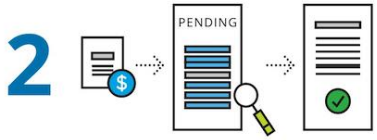


Another view of how blockchain works

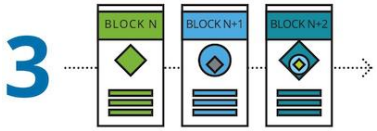
Figure 1. How does blockchain work?

Blockchain allows for the secure management of a shared ledger, where transactions are verified and stored on a network without a governing central authority. Blockchains can come in different configurations, ranging from public, open-source networks to private blockchains that require explicit permission to read or write. Computer science and advanced mathematics (in the form of cryptographic hash functions) are what make blockchains tick, not just enabling transactions but also protecting a blockchain's integrity and anonymity.

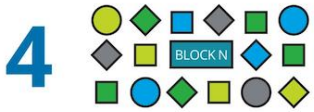
TRANSACTION Two parties exchange data; this could represent money, contracts, deeds, medical records, customer details, or any other asset that can be described in digital form.



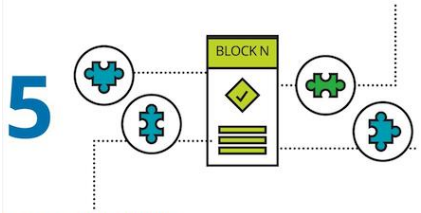
VERIFICATION Depending on the network's parameters, the transaction is either verified instantly or transcribed into a secured record and placed in a queue of pending transactions. In this case, nodes—the computers or servers in the network—determine if the transactions are valid based on a set of rules the network has agreed on.



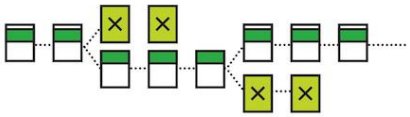
STRUCTURE Each block is identified by a hash, a 256-bit number, created using an algorithm agreed upon by the network. A block contains a header, a reference to the previous block's hash, and a group of transactions. The sequence of linked hashes creates a secure, interdependent chain.



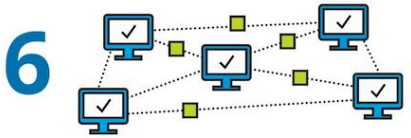
VALIDATION Blocks must first be validated to be added to the blockchain. The most accepted form of validation for open-source blockchains is proof of work—the solution to a mathematical puzzle derived from the block's header.



BLOCKCHAIN MINING Miners try to "solve" the block by making incremental changes to one variable until the solution satisfies a network-wide target. This is called "proof of work" because correct answers cannot be falsified; potential solutions must prove that the appropriate level of computing power was drained in solving.



BUILT-IN DEFENSE If a malicious miner tries to submit an altered block to the chain, the hash function of that block, and all following blocks, would change. The other nodes would detect these changes and reject the block from the majority chain, preventing corruption.

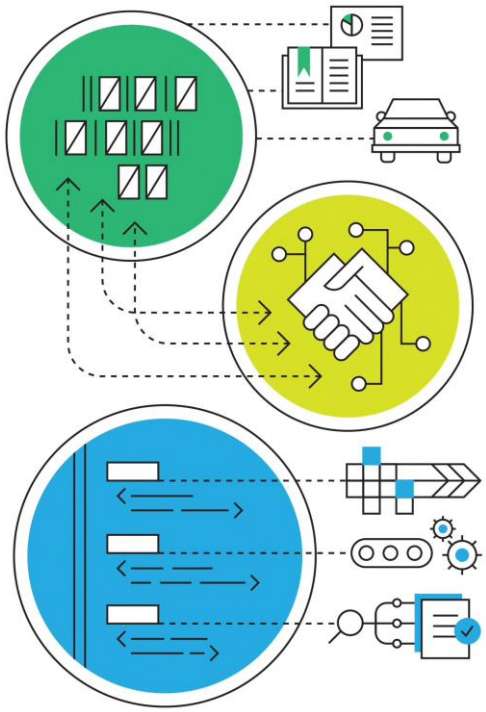


THE CHAIN When a block is validated, the miners that solved the puzzle are rewarded and the block is distributed through the network. Each node adds the block to the majority chain, the network's immutable and auditable blockchain.

Source: Eric Piscini, Joe Guastella, Alex Rozman, and Tom Nassim, *Blockchain: Democratized trust*, Deloitte University Press, February 24, 2016. **Deloitte Insights | deloitte.com/insights**

Blockchain utilization

Figure 2. Three levels of blockchain



1 Storing digital records

Blockchain allows unprecedented control of information through secure, auditable, and immutable records of not only transactions, but also digital representations of physical assets.

2 Exchanging digital assets

Users can issue new assets and transfer ownership in real time without banks, stock exchanges, or payment processors.

3 Executing smart contracts

Self-governing contracts simplify and automate lengthy and inefficient business processes.

Ground rules: Terms and conditions are recorded in the contract's code.

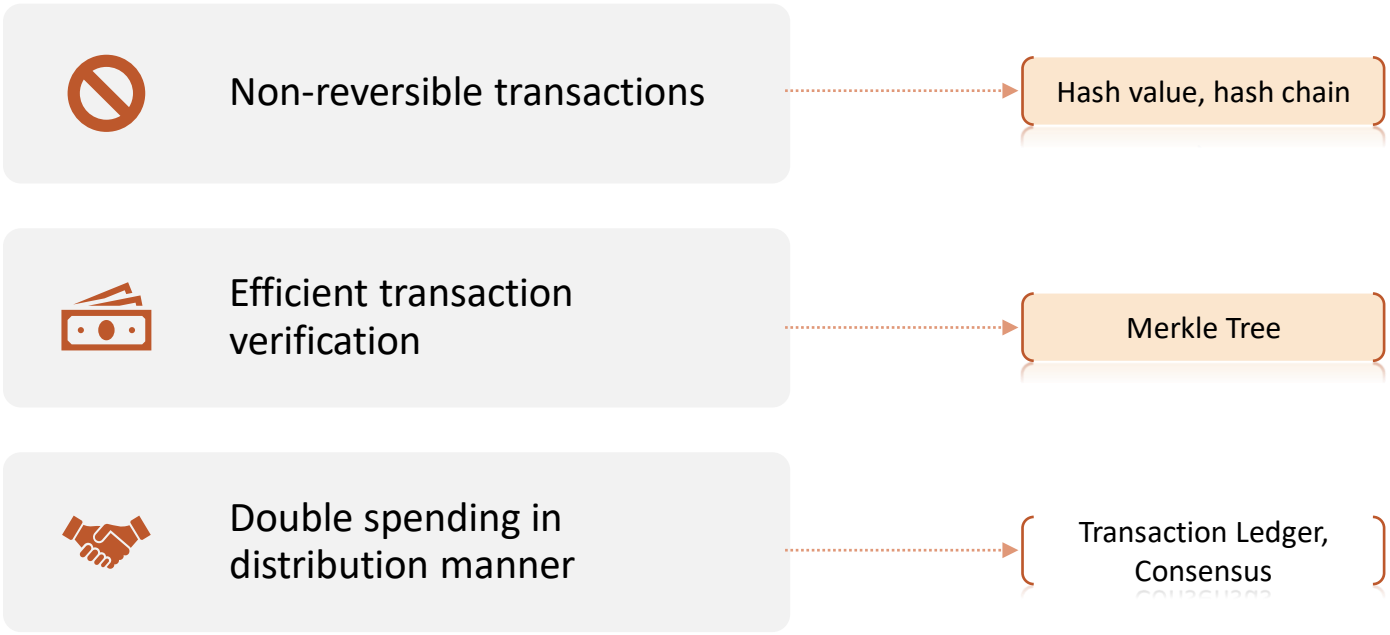
Implementation: The shared network automatically executes the contract and monitors compliance.

Verification: Outcomes are validated instantaneously without a third party.

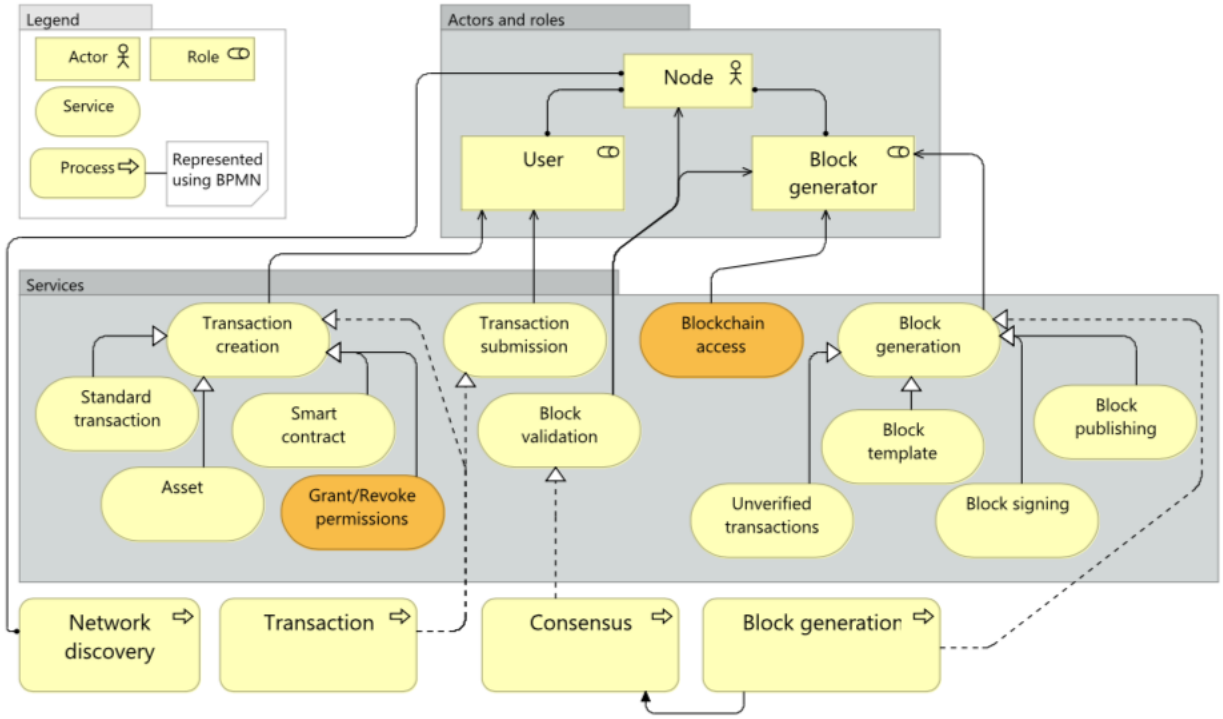
Source: Eric Piscini, Gys Hyman, and Wendy Henry, "Blockchain: Trust economy," *Tech Trends 2017*, Deloitte University Press, February 7, 2017.

Deloitte Insights | deloitte.com/insights

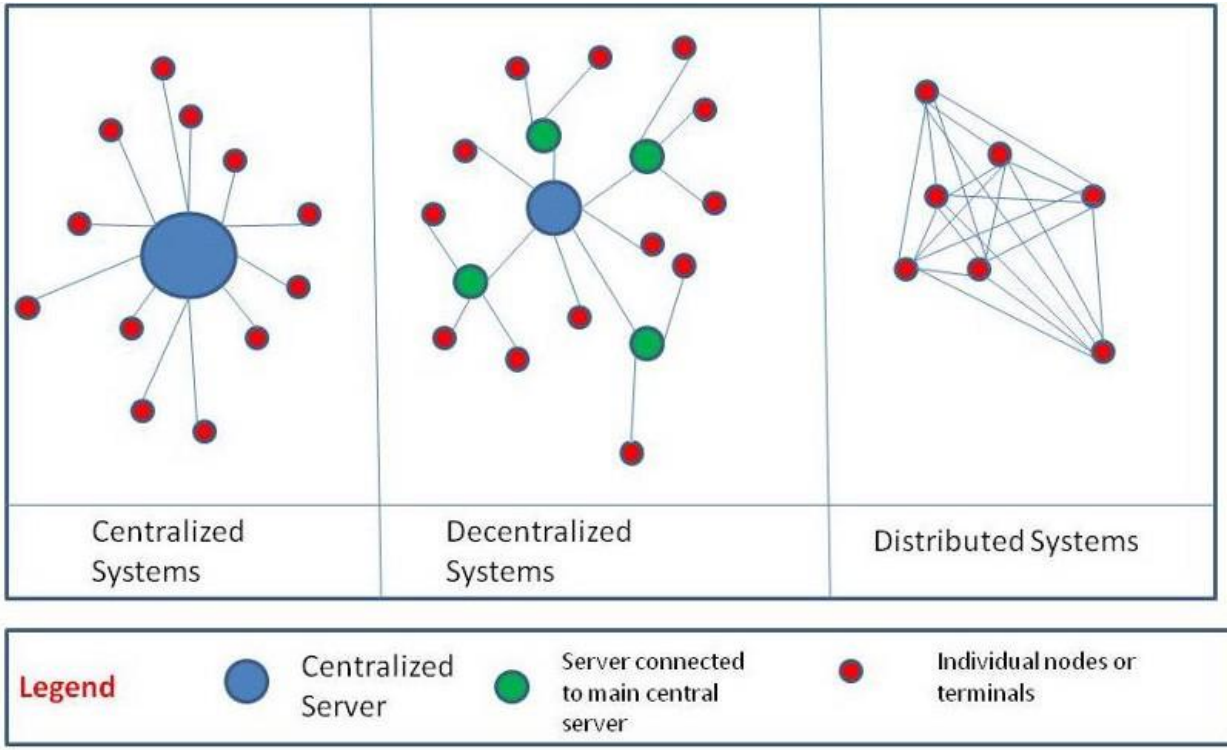
Application of Cryptography to Blockchain



Reference model of the Blockchain Technology



Centralized Vs Decentralized Vs Distributed networks



Types of Blockchain

Types of blockchain

Public blockchain:

- Everyone can check the transaction and verify it and can also participate the process of getting consensus.
- Example: Bitcoin and Ethereum are both Public Blockchain.

Consortium blockchains:

- It means the node that had authority can be choose in advance, usually has partnerships like business to business, the data in blockchain can be open or private, can be seen as Partly Decentralized.
- Example: R3 (banks), EWF (Energy), Hyperledger and R3CEV are both consortium blockchains.

Private blockchain:

- Node will be restricted, not every node can participate this blockchain, has strict authority management on data access.
- Allows only selected entry of verified participants
- A participant can join such a private network only through an authentic and verified invitation

Private vs Public

Public	Private
Transaction ledger disclosed all involved parties of transaction through internet	Private-type Blockchain concept Structure where on management entity can exercise management and authority
Everyone can participate in notarization by using computer power	Emergence of private service
Less likely be exposed to 51% attack	Control over the participants of the network
Higher decentralization level with more nodes	a) Make the network faster and more efficient in the validation of transactions b) Use other consensus mechanisms for more convenient usage
Bitcoin Ethereum	Corda Hyperledger Fabric

Public or private -> any node can join the network to broadcast transactions or mine block? That is whether there an authoritative party?

Permissioned vs Permissionless

Permissionless	Permissioned
Permissionless blockchain networks are decentralized ledger platforms open to anyone publishing blocks, without needing permission from any authority. (NIST) Anybody is allow to participate in the network Any blockchain network user within a permissionless blockchain network can read and write to the ledger	Permissioned blockchain networks are ones where users publishing blocks must be authorized by some authority (NIST) Participants are selected in advance and access to the network is restricted Permissioned blockchain networks may thus allow anyone to read the blockchain or they may restrict read access to authorized individuals They also may allow anyone to submit transactions to be included in the blockchain or, again, they may restrict this access only to authorized individuals
Bitcoin Ethereum	Corda Neo Hyperledger Fabric

Permissioned vs permissionless: Able to run a node with abilities that are unavailable to the general public.

Public vs Private and Permission vs Permissionless

In public blockchains, these transactions are immutably recorded across peered networks using cryptographic trust and assurance mechanisms.

Important blockchain capabilities include tokenization (representation of value or other condition via electronic means) and support for smart contracts (automated execution of actions based on circumstances)

Public blockchains are typically "permissionless" (anyone can join by following the protocol for transacting) and offer anonymity (or pseudoanonymity) for transactions by design.

Most private blockchain-styled blockchains are permissioned, and so, by definition, do not offer anonymity — for example, money transfers must be tracked and identified.

Governance is a critical issue for public blockchains, but less so for private or permissioned blockchains, since it's likely the latter will be governed by the blockchain "organizer."

Private permissionless solutions aim to store contract in its own ad-hoc rather than public chain.

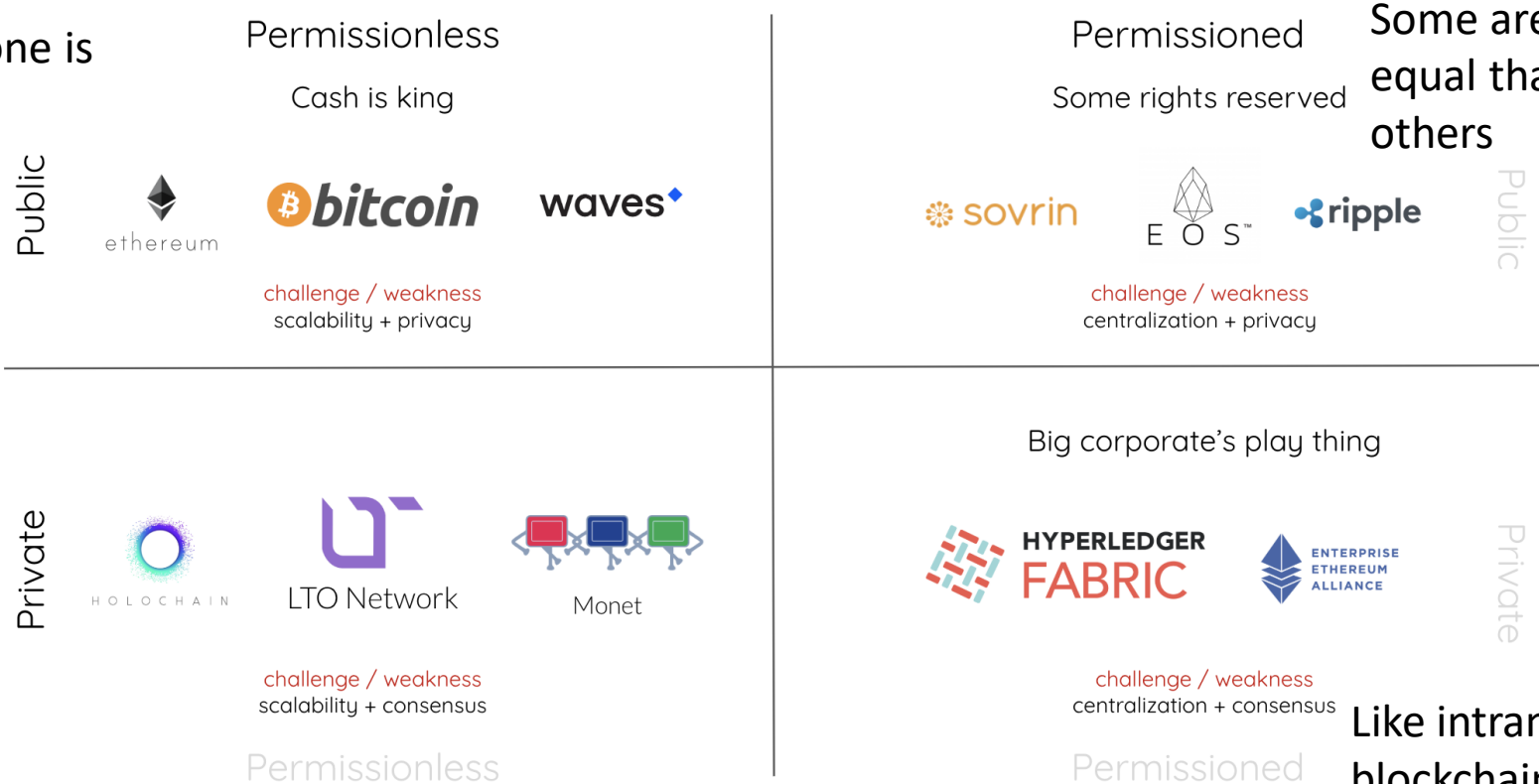
Public	Private
Publish or share data	Publish or share data after authoritative party confirm

Permissionless	Permissioned
Join network (Access Control)	Join network that not publicly available

Permissioned vs Permissionless

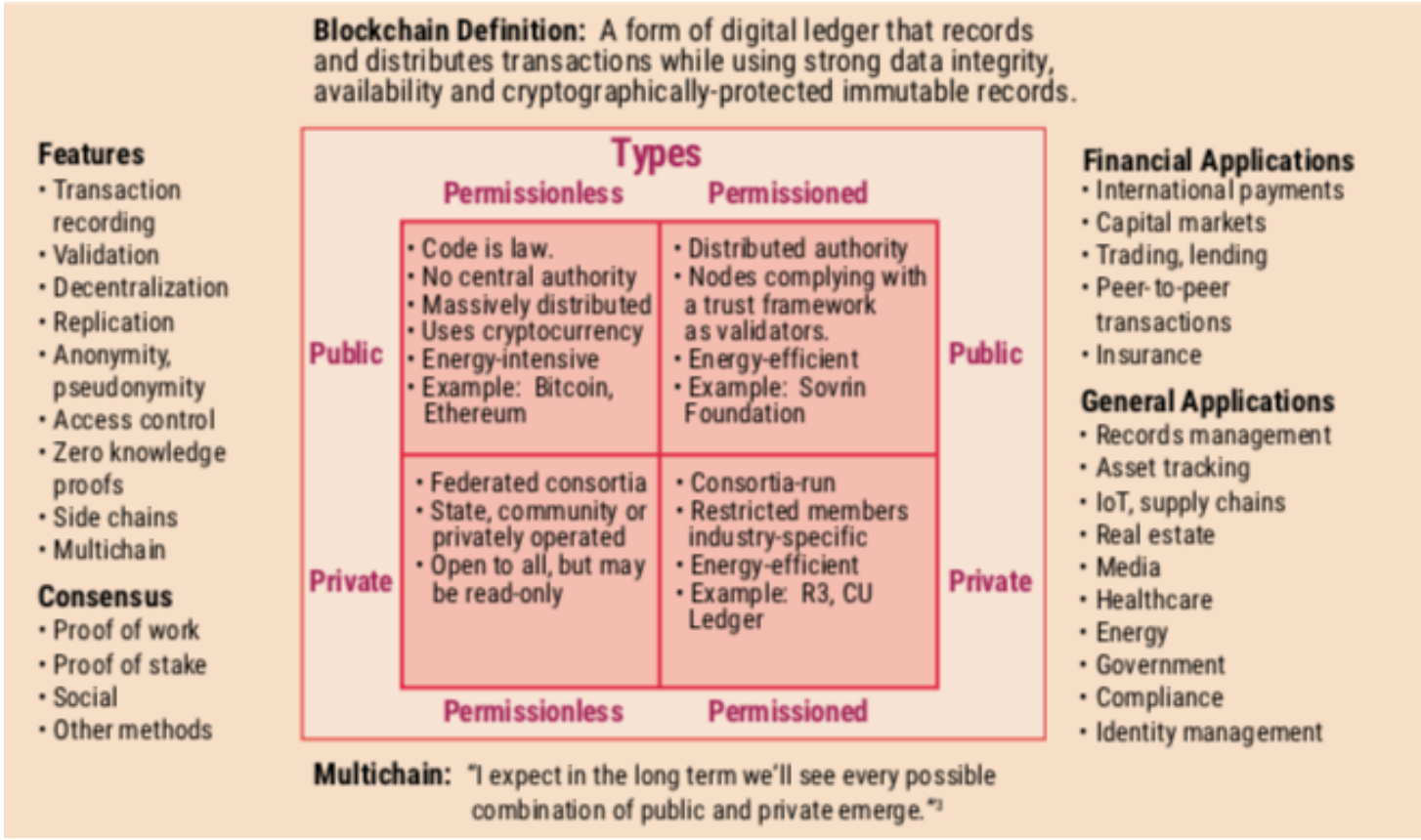
Everyone is equal

Some are more equal than others



Like intranet, but blockchain-isch

Comparison of types of Blockchain technology



Consolidated Comparison of types of Blockchain technology

	Permissionless Public	Permissioned Public	Permissionless Private	Permissioned Private
Consensus protocol (e.g.)	Proof of Work	Proof of Stake	Federated Byzantine Agreement (FBA)	PBFT / Multisignature
Participation	Everyone can connect, download and act as a node	Only users meeting defined criteria can download and act as a node	Everyone in the private network can act as a node	Only selected nodes in private channel can act as a node
Energy Consumption	High	Medium	Low	Low
Immutability	Very High	High	Medium	High
Speed	Very Slow	Slow	Fast	Very fast
Trust Level	Trustless	Trustless	Trusted	Trusted
Anonymity	Pseudo	Pseudo	Known Identity but secret transaction	Known Identity but secret transaction
Scalability	Low	Moderate	Moderate	High
Blockchain (e.g)	Bitcoin, Monero	Bitshares, Ethereum (in future)	Ripper, Stellar	Hyperledger Fabric

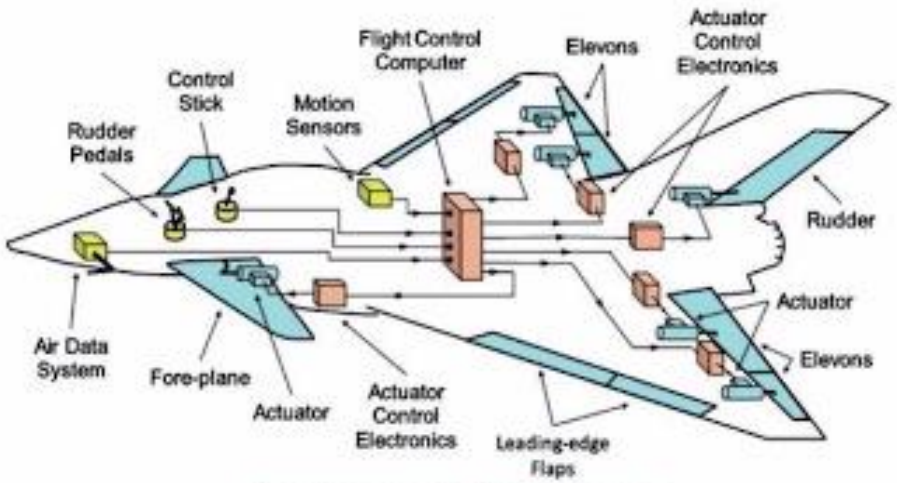
Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" Problems that this paper aim to solve

- Non-reversible transactions
- Efficient transaction verification
- Double spending in distribution manner

Fundamental problems

A fundamental problem in distributed computing and multi-agent systems is to achieve overall system reliability in the presence of a number of faulty processes.

- **What** happens when an actor decides to not follow the rules and to tamper with the state of his ledger?
- **What** happens when these actors are a large part of the network, but not the majority?



Basic elements of the FWB control system.

Consensus Algorithms

A consensus algorithm is a process in computer science used to achieve agreement on a single data value among distributed systems.

Consensus algorithms are designed to achieve reliability in a network involving multiple nodes

Consensus algorithms ensure that the next block in a blockchain is fully validated and secured. There are multiple kinds of consensus algorithms which currently exist, each with different fundamental processes.

Consensus algorithms are capable of doing two things:

- ensuring that the next block in a blockchain is the one and only version of the truth, and
- keeping powerful adversaries from derailing the system and successfully forking the chain.

Consensus Algorithm

How to ensure correctness of a consensus algorithm

Consensus Algorithms

The main reason to implemented consensus algorithm for blockchain is

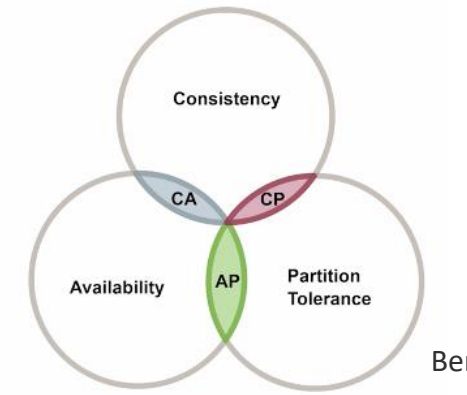
- the network picks up the best decision which should favor for all of them.
- the decision does not give benefits but comes from majority votes means the choice will not implement
- implemented to run a fairness online world
- aims at finding a common agreement that is a win for the entire network.

Consensus Algorithms

Blockchain might well provide the primitives to break CAP and maintain ACID

CAP → **C**onsistency + **A**vailability + **P**artition Tolerance

ACID → **A**tomicity + **C**onsistency + **I**solation + **D**urability



BerkeleyX: CS198.2xBlockchain Technology

CAP Theorem (Definition)

C—Consistency:

- Consensus guarantees only one truth of what happened and in what order
- Every node in a distributed cluster returns the same, most recent, successful write.

A—Availability:

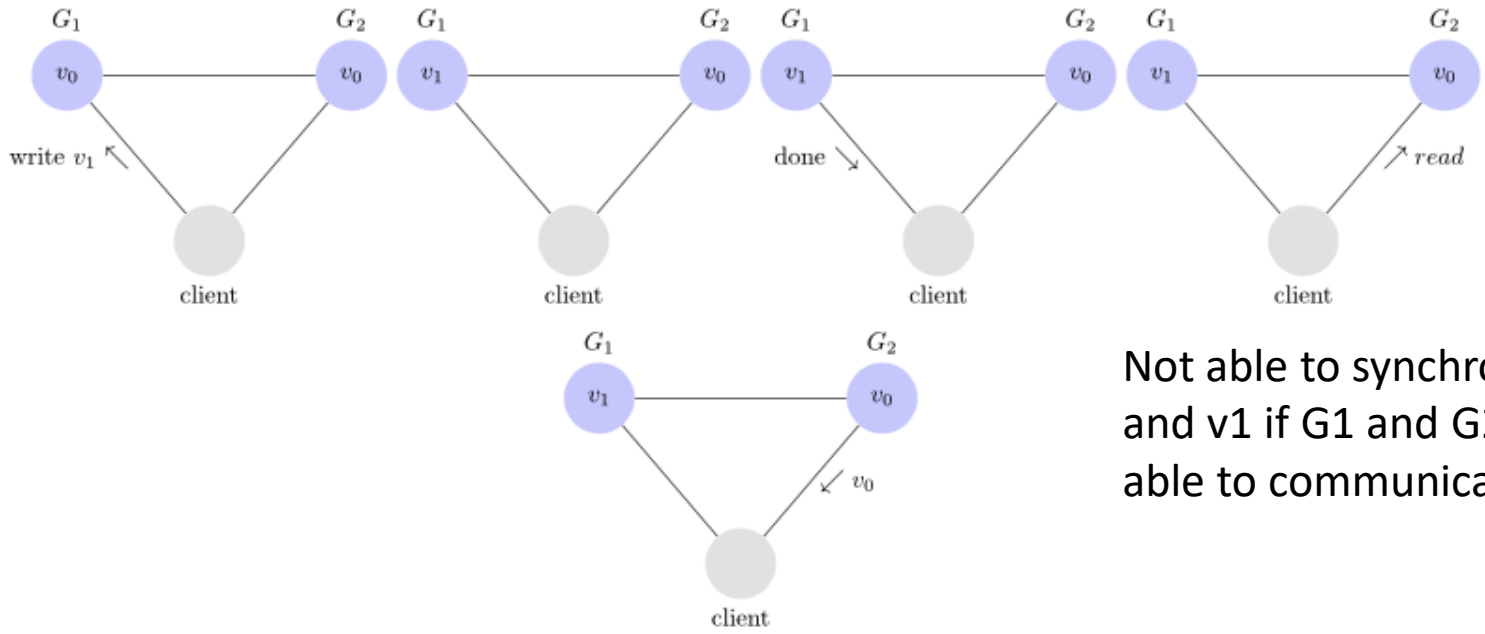
- The fact that all calls to the blockchain are asynchronous allows the invoking application to make progress while ensuring consensus and durability (chaining also guarantees this)
- Every non-failing node returns a response for all read and write requests in a reasonable amount of time
- Every node on (either side of a network partition) must be able to respond in a reasonable amount of time

P—Network partition/Partition Tolerance:

- Consensus, again, prevents split-brain with conflicts when things get back together after a network partition
- Distributed systems guaranteeing partition tolerance can gracefully recover from partitions once the partition heals.

CAP Theorem

Consistency problem



Not able to synchronize v0 and v1 if G1 and G2 not able to communicate

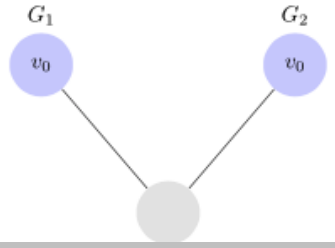
CAP Theorem

Availability (Available of content)

- In an available system, if our client sends a request to a server and the server has not crashed, then the server must eventually respond to the client
- Server is not allowed to ignore the client's requests.

Partition Tolerance (Able to communicate)

- This means that any messages G1 and G2 send to one another can be dropped or delayed but system can still continue to operate.



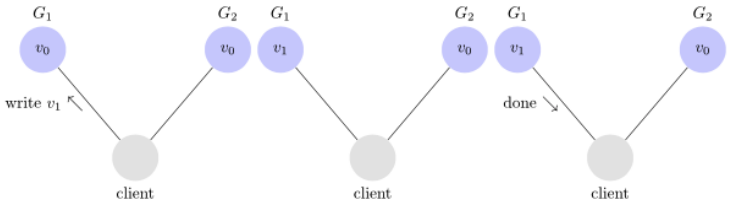
With the notion of consistency, availability, and partition tolerance, we can prove that a system cannot simultaneously have all three.
"only two out of the three promises can be fulfilled"

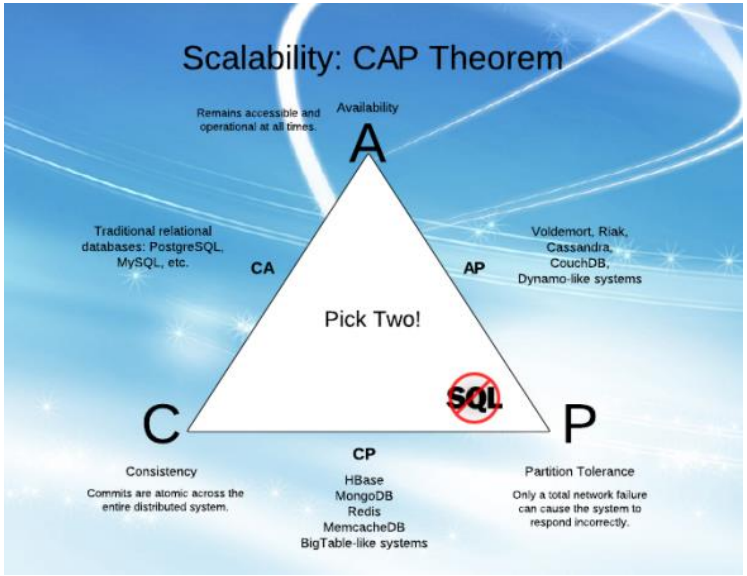
CAP Theorem

Consistency & Availability (CA)
- Without any network partitioning, consistent and availability can be achieved.

Availability & Partition Tolerance (AP)
- Partitioned network and kept available
- Not able to keep consistent

Consistency & Partition Tolerance (CP)
- Consistency kept when partitioned tolerance
- Data is consistent between all nodes, and maintains partition tolerance (preventing data desync) by becoming unavailable when a node goes down.





Consistency vs availability

ACID

- The first version of this consistency-versus-availability argument appeared as ACID versus BASE which was not well received at the time, primarily because people love the ACID properties and are hesitant to give them up

Manage partitions

- Detect partitions, enter an explicit partition mode that can limit some operations, and initiate a recovery process to restore consistency and compensate for mistakes made during a partition.

Fallacies in Distributed Computing Environment

Network is reliable

Latency is zero

Bandwidth is infinite

Network is secure

Topology does not change

Transport cost is zero

Homogeneous network

Trust all

Compensation issues in Automated Teller Machine (ATM)

ATM design serves as a good context for reviewing some of the challenges involved in compensating for invariant violations during a partition.

The ATM system designer could choose to prohibit withdrawals during a partition, since it is impossible to know the true balance at that time, but that would compromise availability.

The ATM chooses a sophisticated limit on availability that permits withdrawals but bounds the risk.

Restoring state is easy because the operations are commutative, but compensation can take several forms. A final balance below zero violates the invariant.

The banking system depends not on consistency for correctness, but rather on auditing and compensation

Consensus Algorithms (Problem)

C—Consistency:
- Consensus guarantees only one truth of what happened and in what order

A—Availability:
- The fact that all calls to the blockchain are asynchronous allows the invoking application to make progress while ensuring consensus and durability (chaining also guarantees this)

P—Network partition/Partition Tolerance:
- Consensus, again, prevents split-brain with conflicts when things get back together after a network partition

A—Atomicity:
- The chaincode programming model is an all-or-nothing behavior, which allows you to group activities together. Either everything happens, or it doesn't.

C—Consistency:
- We believe the new world of NoSQL fudges this one. I believe this means the same as the *C* in CAP.

I—Isolation:
- Isolation indicates that two transactions are serialized, which is exactly what block construction and chaining does.

D—Durability:
- The chaining and replication all over the network ensures that if one or more nodes go down, data won't be lost. This is why everyone wants to bring a node and why those nodes should not be not co-located.

Consensus Algorithms

Block adder

Validator

Byzantine General's Problem

Byzantine General's Problem

- Byzantine Generals' Problem, a dilemma that has been extensively researched and optimized with a diverse set of solutions in practice and actively being developed.
- Circling back to the Byzantine Generals' Problem, which is what set this system in motion, there have been many specifications and improvements made to the overall algorithm since the overarching problem has been studied and analyzed for years now.

Byzantine General's Problem

This problem (first published in 1975 and given its name in 1978) describes a scenario where two generals are attacking a common enemy. Described in 1982 by Lamport, Shostak and Pease, it is a generalized version of the Two Generals Problem with a twist.

Each general's army on its own is not enough to defeat the enemy army successfully, thus they need to cooperate and attack at the same time

General 1 has to send a messenger across the enemy's camp that will deliver the time of the attack to General 2.

However, there is a possibility that the messenger will get captured by the enemies and thus the message won't be delivered.

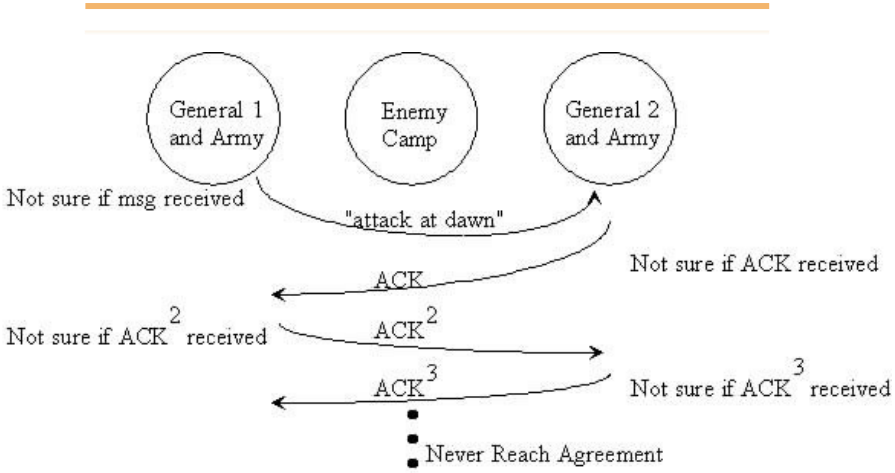
There is no way to guarantee the second requirement that each general be sure the other has agreed to the attack plan.

Byzantine General's Problem

If all generals and/or messengers were trustworthy then it is a very simple solution.

However, some of the messengers and even a few generals/commanders are traitors. They are spies or even enemy soldiers.

There is a very high chance that they will not follow orders or pass on the incorrect message.



The Two Generals Problem has been proven to be unsolvable.
The algorithm to reach consensus in this case is based on the value of majority of the decisions a lieutenant observes.

Consensus Algorithms

There are several different kinds of consensus algorithms

	PoW	PoS	PoET	BFT and variants	Federated BFT
Blockchain type	Permissionless	Both	Both	Permissioned	Permissionless
Transaction finality	Probabilistic	Probabilistic	Probabilistic	Immediate	Immediate
Transaction rate	Low	High	Medium	High	High
Token needed?	Yes	Yes	No	No	No
Cost of participation	Yes	Yes	No	No	No
Scalability of peer network	High	High	High	Low	High
Trust model	Untrusted	Untrusted	Untrusted	Semi-trusted	Semi-trusted
Adversary Tolerance	<=25%	Depends on specific algorithm used	Unknown	<=33%	<=33%

Consensus Algorithm

Achieve the agreement based on probability instead of exact agreement

Objectives of Blockchain consensus models

- Coming to an agreement
- Collaboration
- Co-operation
- Equal Rights
- Participation
- Activity

Soul of the Consensus Algorithms

- Nodes not required to be trusted
- Trust is based on incentives

Proof of Work

Proof of Work algorithm

- Used to process blocks of transactions and add them to the blockchain
- Utilized for block generation
- Compete for scarce resources – Computational Power.
- The process of generating correct proofs in order to add a block to the blockchain is known as "mining" and the individuals that participate in the mining process are known as "miners."
- Distributed and trustless consensus algorithm is Bitcoin's proof-of-work (PoW) algorithm
- PoW requires miners to solve complex cryptographic puzzles before they can add a block to the blockchain.
- Proof of Work provides a probabilistic solution to the Byzantine Generals Problem

With proof of work, miners who find the correct hash are allowed to generate new blocks and are rewarded for doing so.

Proof of Work – Mathematical Puzzle

There are a lot of them, for instance:

- hash function, or how to find the input knowing the output.
- integer factorization, in other words, how to present a number as a multiplication of two other numbers.
- guided tour puzzle protocol. If the server suspects a DoS attack, it requires a calculation of hash functions, for some nodes in a defined order. In this case, it's a 'how to find a chain of hash function values' problem.

As an example, consider a puzzle where, using the SHA-256 algorithm, a computer must find a hash value meeting the following target criteria (known as the difficulty level):

- SHA256("blockchain" + Nonce) = Hash Digest starting with "000000"

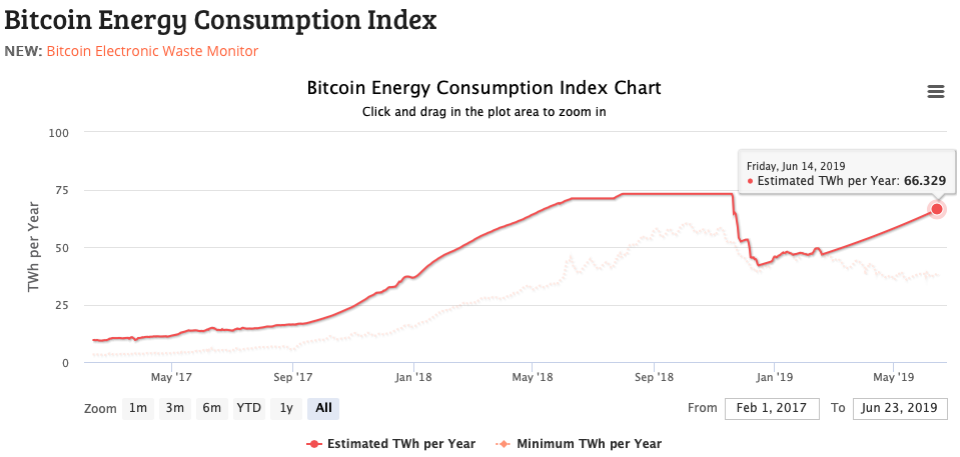
```
SHA256("blockchain0") =
0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938
(not solved)

SHA256("blockchain1") =
0xdb0b9c1cb5e9c680dfff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10
(not solved)

…

SHA256("blockchain10730895") =
0x000000ca1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587
(solved)
```

To solve this puzzle, it took 10,730,896 guesses (completed in 54 seconds on relatively old hardware, starting at 0 and testing one value at a time).

Proof of Work

Operating proof of work systems such as Bitcoin requires a tremendous amount of energy.

In fact, it's estimated that roughly 6.5 million U.S. households could be powered by the energy that is consumed from operating Bitcoin



https://digiconomist.net/bitcoin-energy-consumption

Proof of Work

Popular Implementations: Bitcoin, Ethereum, Litecoin, Dogecoin

Pros: We know it works

Cons: Slow throughput; high energy consumption

In PoW, miners solve hard, useless problems to create blocks. PoW runs on a system of "the longest chain wins." So assuming most miners are working on the same chain, that one will grow fastest will be the longest and most trustworthy

What is the meaning of Stake

A share or a financial involvement in something such as a business:

- He holds (= owns) a 40 percent stake in/of the company.

Have a stake in something

- If you have a stake in something, it is important to you because you have a personal interest or involvement in it: Employers have a stake in the training of their staff.

Proof of Stake (PoS) is a consensus algorithm that depends on both randomization of and vested interest in the blockchain.
Compete for scarce resources – Cryptocurrency (Stake)
The cryptocurrency must be owned without used.

What is Proof of Stake

The idea of the Proof of Stake (PoS) consensus was propounded by Scott Nadal and Sunny King in 2012.

In PoS, computational power is replaced by currency power. It depends on the number of tokens a node has in its wallet.

In other words, ability to validate a transaction depends on how much 'stake' one has in the network.

There will be no block rewards but only the transaction fee.

New coins will not be mined.

Proof of Stake

Proof of Stake (PoS) consensus algorithm

- Another way to generate blocks within a blockchain, differing from that of the Proof of Work algorithm.
- Individuals that are chosen to generate a block, also known as validators, depend on a different set of criteria.
- A validator is chosen **at random** to generate a new block based on their economic stake in the network
- Validators are selected to generate a new block with a probability that is proportional to the amount of coins that the validator possesses.
- The more coins a validator houses in his wallet, the increased likelihood of being selected to generate a block. Some proof of stake systems also take into account the length of time (coin age) that a validator has held coins in their wallet.
- Proof of stake is seen as being a superior block generating mechanism to proof of work because of reasons primarily pertaining to energy consumption

Proof of Stake

Relative value: The relative value of coins held in the validator's wallet, which is equal to: the total value of coins in the validator's wallet divided by the total value of coins on the network

With proof of stake, a validator generates a new block by sending a special type of transaction that locks up their deposit. This deposit (or stake) serves as collateral for the block generation process.

In this scenario, validators are incentivized to form blocks on top of both competing chains just to be sure that they are backing the chain that will eventually win out.

Need to create blocks when chosen and validate proposed blocks when they're not. Validators get rewards for proposing new blocks and for attesting to ones they've seen.

If you attest to malicious blocks, you lose your stake.

Proof of Stake

The Proof of Stake (PoS) algorithm utilizes validators who are chosen based on criteria that includes coin age and economic stake. PoS also requires significantly less energy thanks to its validator selection criteria.

Proof-of-Stake algorithms achieve consensus by requiring users to stake an amount of their tokens so as to have a chance of being selected to validate blocks of transactions, and get rewarded for doing so.

In PoS the miner of a new block, in this case known as the forger, is chosen in a semi-random, two-part process.

Every validator must own a stake in the network. Staking involves depositing an amount of tokens into the system, locking it in what you can think of as a virtual safe, and using it as a collateral to vouch for the block.

The key here is to include a degree of chance to the selection process so as to avoid a scenario where the richest users are always selected to validate transactions, consistently reap the rewards and grow richer and richer.

Forgers are selected by looking for users with a combination of the lowest hash value and highest stakes.

Proof of Stake

In PoS, the blocks aren't created by miners doing work, but by minters staking their tokens to "bet" on which blocks are valid.

In the case of a fork, minters spend their tokens voting on which fork to support. Assuming most people vote on the correct fork, validators who voted on the wrong fork would "lose their stake" in the correct one.

The concern is that since it costs validators almost no computational power to support a fork unlike PoW, validators could vote for both sides of every fork that happens

Popular implementations:

- Decred, Ethereum and Peercoin

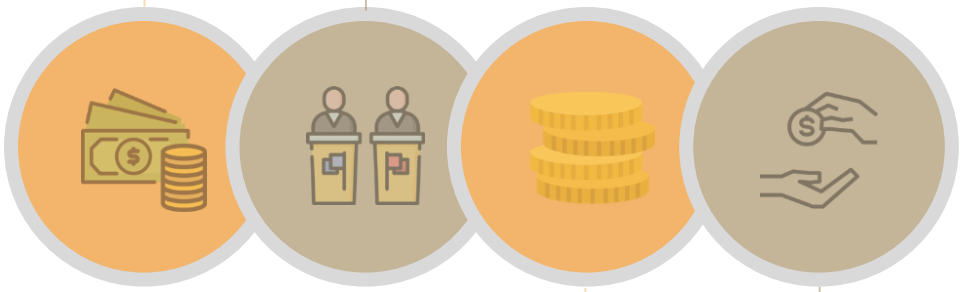
Pros: Attacks more expensive; More decentralized; Energy efficient

Method for different ways of Stake to be selected

Four different ways of use of Stake

Random selection of staked users
(Chain-based proof of stake)

Multi-round voting



Coin Aging Systems

Delegate Systems

Chain-based Proof of Stake

A proof of stake consensus model where the blockchain network decides the next block through pseudo-random selection, based on a personal stake to overall system asset ratio.

Random selection of staked users

The blockchain network will look at all users with stake and choose amongst them based on their ratio of stake to the overall amount of cryptocurrency staked.

So, if a user had 42 % of the entire blockchain network stake they would be chosen 42 % of the time; those with 1 % would be chosen 1 % of the time.

Focus on the validator

Multi-round voting Proof of Stake

Also known as Byzantine Fault Tolerance Proof of Stake

A proof of stake consensus model where the blockchain decides the next block by allowing all staked members to "vote" on which submitted block to include next.

The blockchain network will select several staked users to create proposed blocks.

Then all staked users will cast a vote for a proposed block.

Several rounds of voting may occur before a new block is decided upon.

This method allows all staked users to have a voice in the block selection process for every new block.

Popular implementations:

- Hyperledger, Stellar, Dispatch and Ripple

Pros: High throughput; low cost; scalable

Cons: Semi-trusted

Coin age proof of stake

Staked cryptocurrency has an age property

The staked cryptocurrency can count towards the owning user being selected to publish the next block.

The staked cryptocurrency then has its age reset, and it cannot be used again until after the requisite time has passed.

To prevent stakeholders from hoarding aged cryptocurrencies, there is generally a built-in maximum to the probability of winning.

Delegated Proof-of-Stake (DPoS)

DPoS is developed by Daniel Larimer, and is actually very different from PoS.

Users vote for nodes to become publishing nodes – therefore creating blocks on their behalf.

There are generally between 21–100 elected delegates in a DPoS system.

In DPoS, token holders don't vote on the validity of the blocks themselves, but vote to elect delegates to do the validation on their behalf.

Nodes who receive the most votes become publishing nodes and can validate and publish blocks. Thus, miners can collaborate to make blocks instead of competing like in PoW and PoS.

If delegates continually miss their blocks or publish invalid transactions, the stakers vote them out and replace them with a better delegate.

By partially centralizing the creation of blocks, DPoS is able to run orders of magnitude faster than most other consensus algorithms

Popular Implementations: Steemit, EOS, BitShares

Pros: Cheap transactions; scalable; energy efficient

Cons: Partially centralized

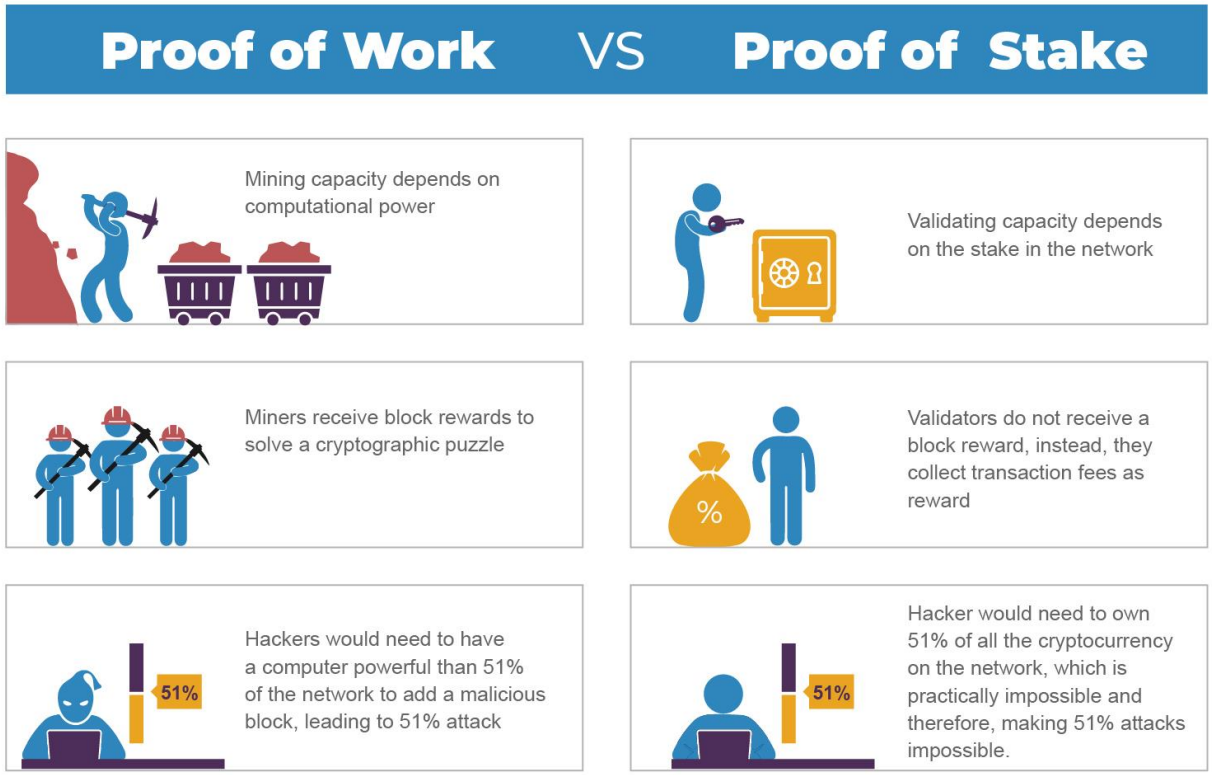
Proof of Stake

Proof of stake breaks this symmetry by relying not on rewards for security, but rather penalties.

Validators put money ("deposits") at stake, are rewarded slightly to compensate them for locking up their capital and maintaining nodes and taking extra precaution to ensure their private key safety, but the bulk of the cost of reverting transactions comes from penalties that are hundreds or thousands of times larger than the rewards that they got in the meantime.

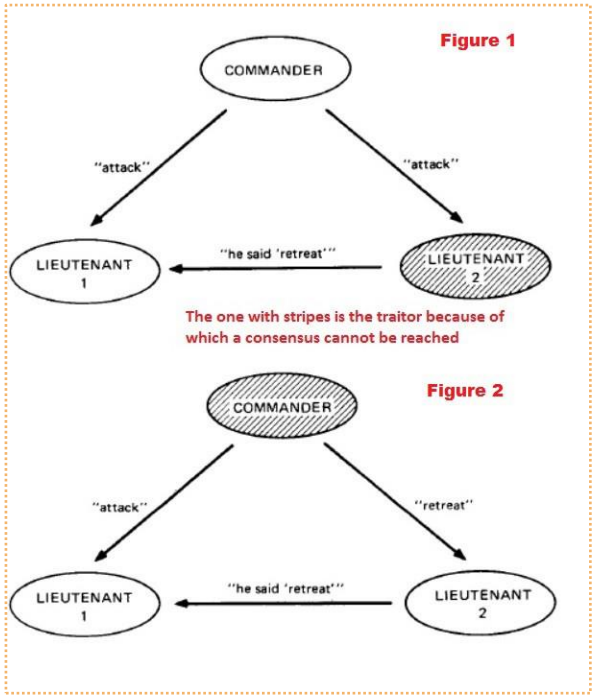
Proof of stake algorithms work on the assumption that people with staked tokens in a network will be incentivized to act in the network's interest

Proof of Work vs Proof of Stake



Byzantine Fault Tolerance

Byzantine Fault Tolerance is the characteristic which defines a system that tolerates the class of failures that belong to the Byzantine Generals' Problem.

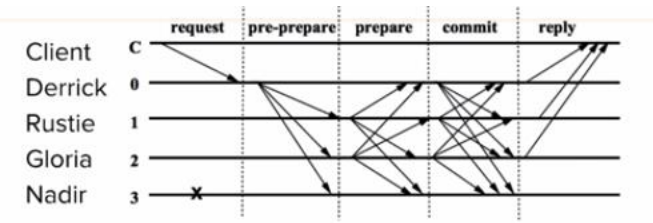


https://www.youtube.com/watch?time_continue=14&v=VWG9xcwjxUg

Byzantine Fault Tolerance

Practical Byzantine Fault Tolerance (PBFT)

- By Miguel Castro and Barbara Liskov
- One of the first solutions to this problem was coined Practical Byzantine Fault Tolerance. Currently in use by Hyperledger Fabric, with few (< 20, after that things get a little) pre-selected generals PBFT runs incredibly efficiently
- High transaction throughput
- Centralized/permissioned

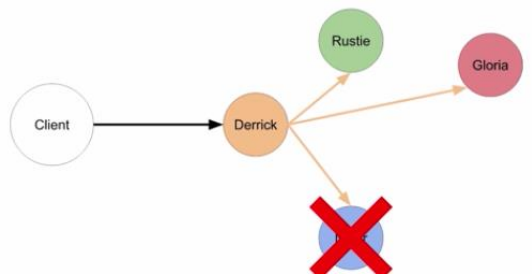


pBFT requires:

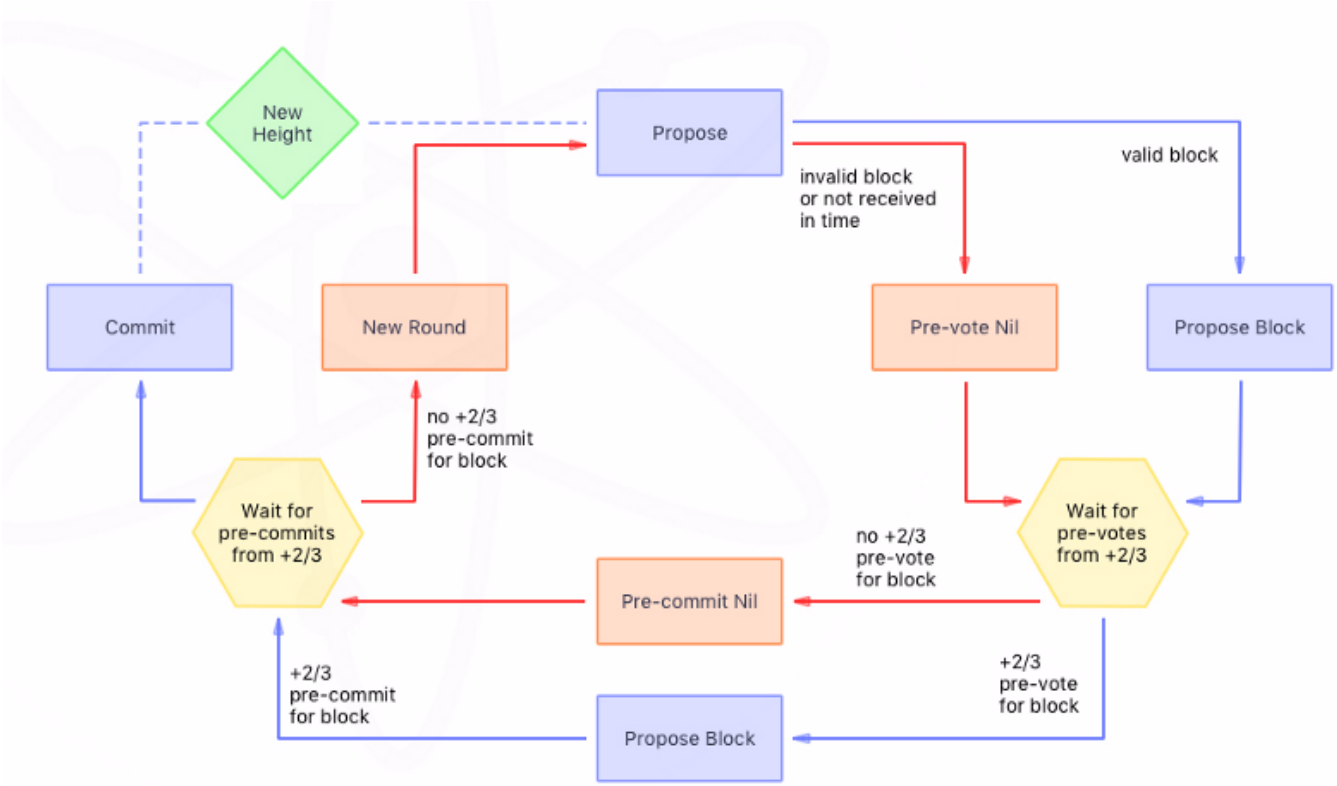
N ≥ 3f + 1

Federated Byzantine Agreement (FBA)

- FBA is another class of solutions to the Byzantine generals problem used by currencies like Stellar and Ripple.
- The general idea, is that every Byzantine general, responsible for their own chain, sorts messages as they come in to establish truth.



Classical BFT consensus algorithm - Tendermint



Tendermint consensus process

Simplified Byzantine Fault Tolerance (SBFT)

The Simplified Byzantine Fault Tolerant consensus algorithm implements an adopted version of the Practical Byzantine Fault Tolerant (PBFT) algorithm

- Single validator given the permissioned nature of the ledger
- In order to be tolerant of a Byzantine fault, the number of nodes that must reach consensus is 2f+1 in a system containing 3f+1 nodes, where f is the number of faults in the system. For example, if we have 7 nodes in the system, then 5 of those nodes must agree if 2 of the nodes are acting in a faulty manner.

Proof of Elapsed Time

Proof of elapsed time (POET) is a blockchain network consensus mechanism algorithm that prevents high resource utilization and high energy consumption and keeps the process more efficient by following a fair lottery system.

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.

In each round of consensus, network participants receive a signed timer object from the trusted code which is completely randomized.

PoET comes from Intel, and it relies on a special CPU instruction set called Intel Software Guard Extensions (SGX). SGX allows applications to run trusted code in a protected environment.

PoET is now the consensus model adopted by Hyperledger Sawtooth's modular framework

PoET, random peers are selected to execute requests at a predetermined rate. The peer with the smallest sample wins the election and gets to commit the block.

Proof of Burn

The Proof of Burn (PoB) algorithm utilizes miners who send their coins to an unspendable address ("eater address"), effectively "burning" the coin forever.

- The entire idea behind proof-of-burn consensus is that the user burning the cryptocurrency shows long-term commitment to the coin by burning it, while receiving his or her gains much later.
- Proof of Burn (PoB) algorithm which works in a fairly simple fashion.
- The miners of the PoB coins will send coins to an unspendable address

These transactions are recorded on the blockchain, ensuring that there's a necessary proof that the coins cannot be spent again, and the user who burned the coins is issued a reward

The entire idea behind proof-of-burn consensus is that the user burning the cryptocurrency is showing long-term commitment to the coin by burning it.

The user of a proof-of-burn coin continues receiving rewards, either increasing their stake of alternative coins or earning greater privileges for mining on the network

Proof-of-Authority (PoA) — Trust the know it all

Proof-of-Authority is a consensus algorithm where transactions are validated by approved accounts, kind of like the “admins” of the system.

A set of “authorities” — nodes that are explicitly allowed to create new blocks and secure the blockchain. A validator is not required to hold a stake in the network.

It is revised from PoS. Validators in PoA systems are known entities that put their reputations on the line for the right to validate the blocks.

PoA is commonly used for private block- chains that are hidden within internal networks.

Popular Implementations: POA.Network, Ethereum Kovan testnet

Pros: High throughput; scalable

Cons: Centralized system

PoA has high throughput, and is optimized for private networks.

Proof-of-Weight (PoWeight) — Bigger is better

Proof-of-Weight is a broad classification of consensus algorithms based around the Algorand consensus model.

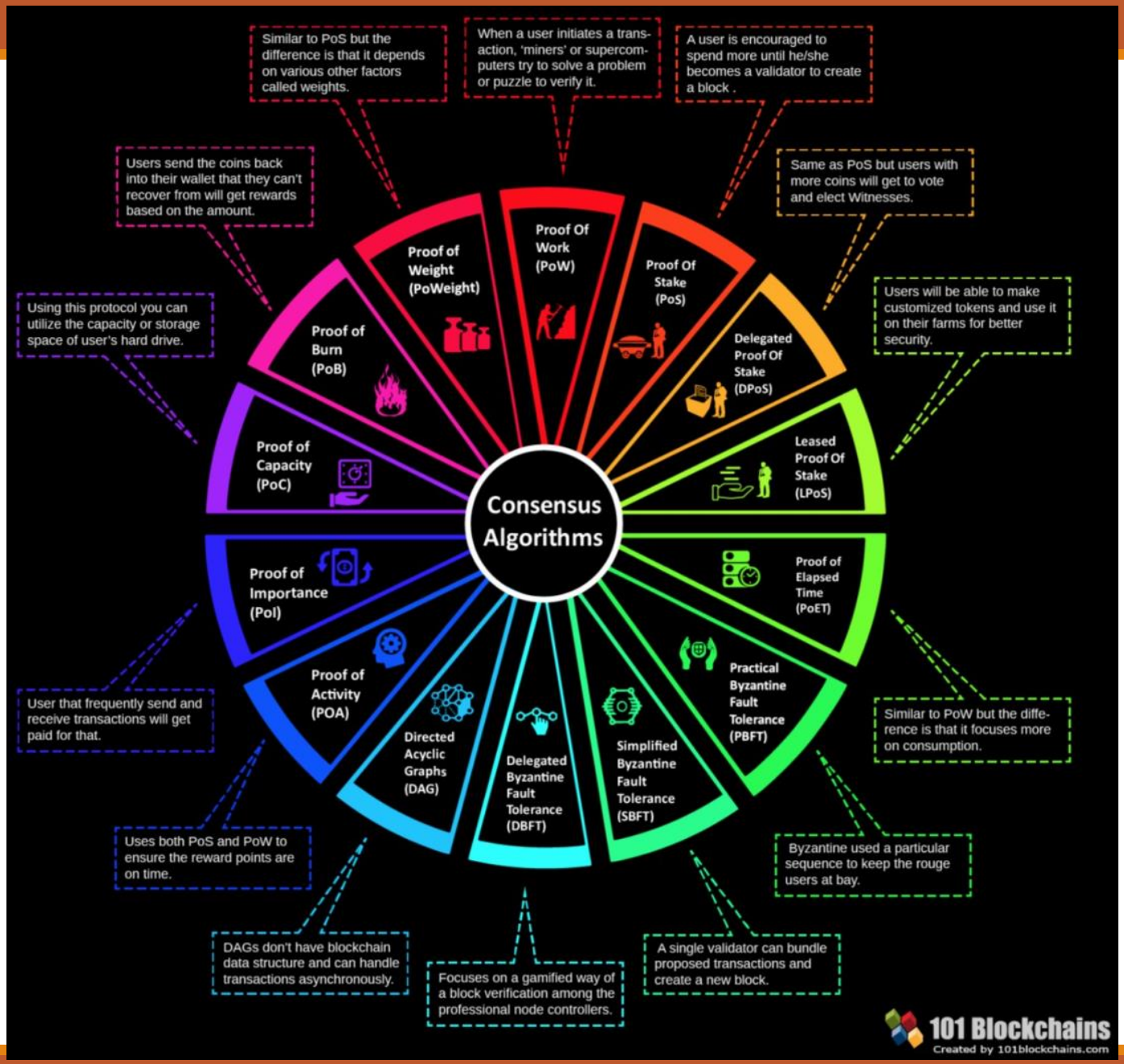
The general idea is that where in PoS, your percentage of tokens owned in the network represents your probability of “discovering” the next block, in a PoWeight system, some other relatively weighted value is used.

Popular Implementations: Algorand, Filecoin, Chia

Pros: Customizable; scalable

Cons: Incentivization can be a challenge

Concrete example: Filecoin’s Proof-of-Spacetime is weighted on how much IPFS data you’re storing. Other systems could include weights for things like Proof-of-Reputation.



Consensus Algorithm Comparison

Consensus Algorithm	Actions activities
Proof of Work	Miners as validator to sign the block.
Proof of Stake	Select a validator (based on X) to sign the block based on the size of “locked cryptocurrency”
Delegated PoS	Users with more coins will get vote and elect witnesses. Select from the PoS pool
Leased Proof of Stake	Many nodes with very few tokens can lease tokens to other nodes, thus forming a joint force and increasing the probability of becoming the validator
Proof of Elapsed Time	The participant who has finished his/her fair share of waiting time will get to be on the ledger to create a new block.
Practical Byzantine Fault Tolerance	PBFT mainly focuses on the state machine.
Simplified Byzantine Fault Tolerance	A block generator will collect all the transactions at a time and validate them after batching them together in a new type of block.

https://www.alibabacloud.com/blog/from-distributed-consensus-algorithms-to-the-blockchain-consensus-mechanism_595315
https://101blockchains.com/consensus-algorithms-blockchain/?spm=a2c65.11461447.0.0.4c15478eNV2ayk

Consensus Algorithm Comparison

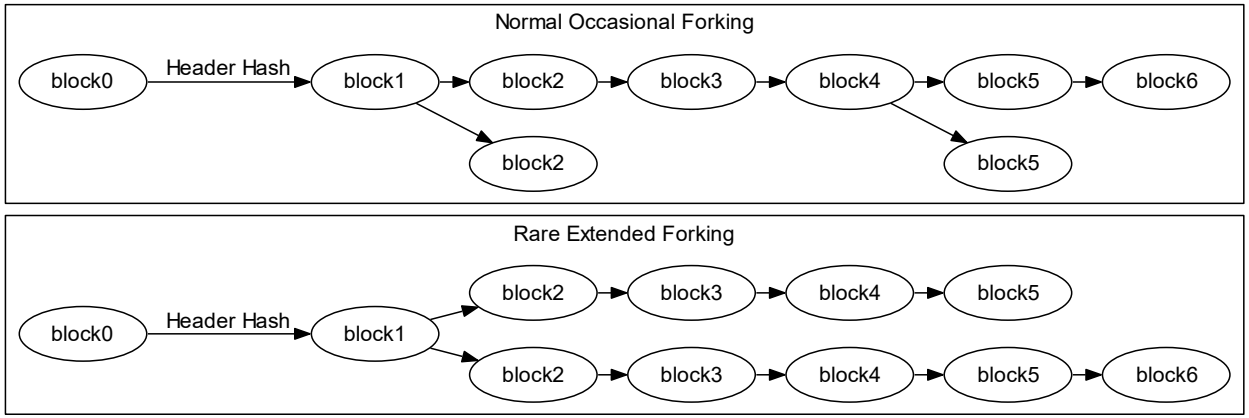
Consensus Algorithm	Actions activities
Delegated Byzantine Fault Tolerance	Focuses on a gamified way of a block verification among the professional node controllers. Based on algo.
Directed Acyclic Graphs (DAG)	DAGs can handle transactions asynchronously.
Proof of Authority (PoA)	A consensus algorithm where transactions are validated by approved accounts, kind of like the “admins” of the system
Proof of Activity (PoA)	PoA combines both PoW and PoS ideas.
Proof of Importance (PoI)	User that frequently send and receive transactions will get paid for that.
Proof of Capacity (PoC)	Known as Proof of Space (PoS). Measured by storage space instead of CPU computational power
Proof of Burn (PoB)	Miners must burn a certain amount of tokens, which means transferring a certain amount of tokens to an eater address
Proof of Weight (PoWeight)	Similar to PoS, but depends on various other factors called weights

https://www.alibabacloud.com/blog/from-distributed-consensus-algorithms-to-the-blockchain-consensus-mechanism_595315
https://101blockchains.com/consensus-algorithms-blockchain/?spm=a2c65.11461447.0.0.4c15478eNV2ayk

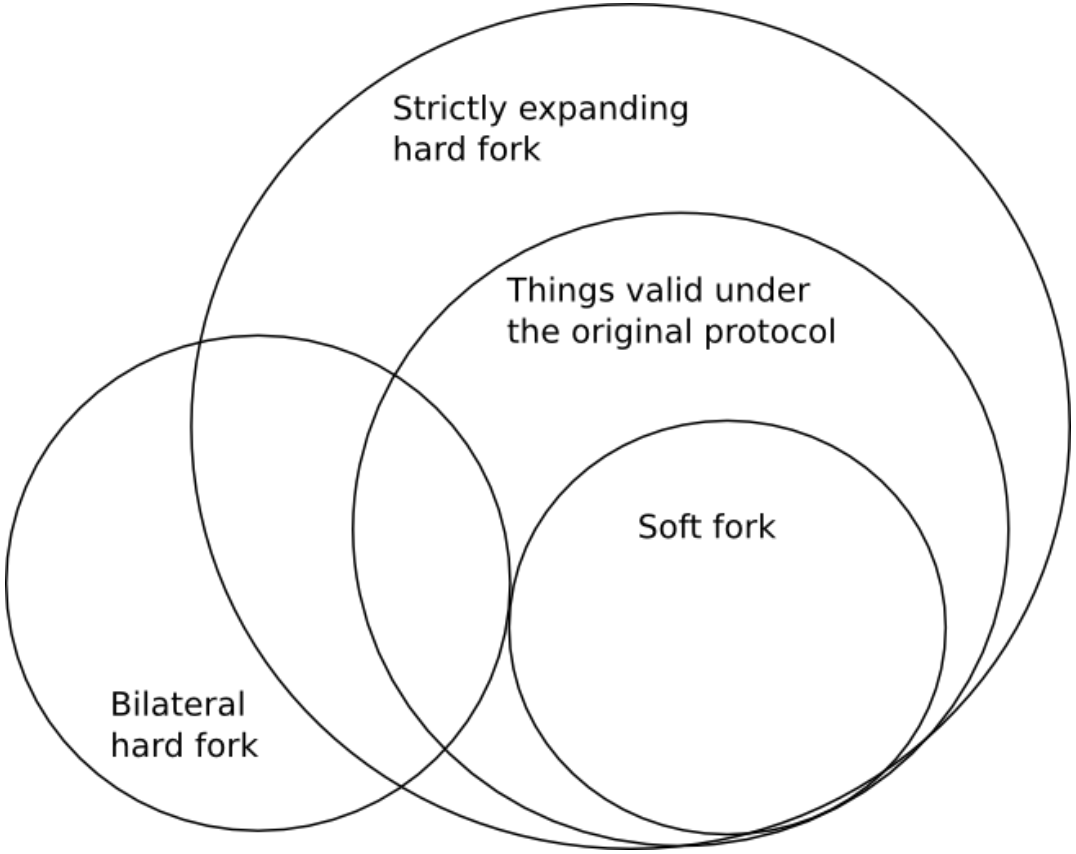
Block Height and Forking

These blocks are commonly addressed by their block height—the number of blocks between them and the first Bitcoin block (block 0, most commonly known as the genesis block).

Multiple blocks can all have the same block height, as is common when two or more miners each produce a block at roughly the same time. This creates an apparent fork in the block chain, as shown in the illustration above.

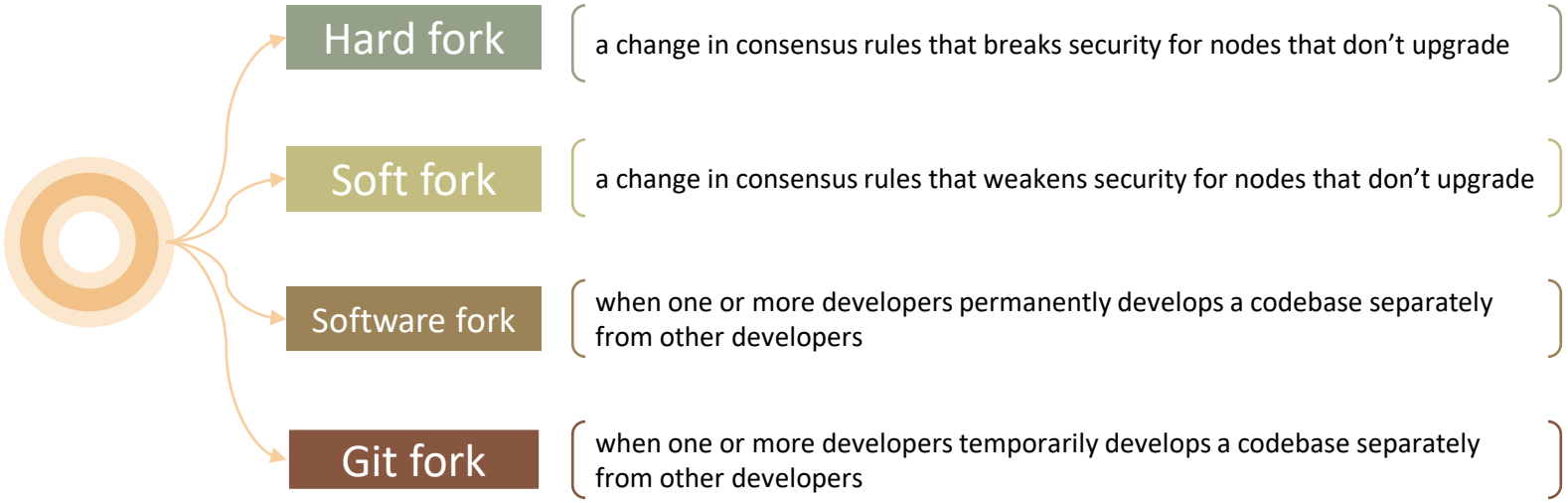


Hard and Soft Fork



Fork

Changes to a blockchain network's protocol and data structures are called **forks.**



Hard Fork

A hard fork, these changes are not backwards compatible because the nodes that have not been updated will reject the blocks following the changes

All publishing nodes will need to switch to using the updated protocol

Non-updated nodes cannot continue to transact on the updated blockchain because they are programmed to reject any block that does not follow their version of the block specification.

User nodes that have not updated will reject the newly formatted blocks and only accept blocks with the old format. This results in two versions of the blockchain existing simultaneously.

Example of hard fork is from Ethereum's DAO incident

Soft Fork

A soft fork, these changes are backwards compatible with nodes that have not been updated.

Non-updated nodes can continue to transact with updated nodes.

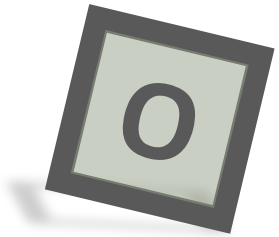
A soft fork occurred on Bitcoin when a new rule was added to support escrow and time-locked refunds.

For nodes that implement this change, the node software will perform this new operation, but for nodes that do not support the change, the transaction is still valid, and execution will continue as if a NOP

Other blocks from fork

Stale block

- Blocks which were successfully mined but which aren't included on the current best block chain, likely because some other block at the same height had its chain extended first.



Orphan block

- Blocks whose parent block has not been processed by the local node, so they can't be fully validated yet.

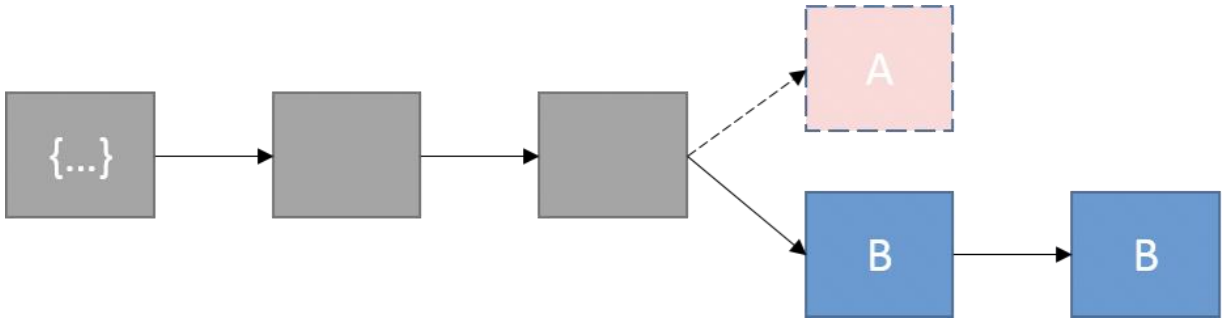
Ledger Conflicts and Resolutions

This depends on network latency between nodes and the proximity of groups of nodes. Permissionless blockchain networks are more prone to have conflicts due to their openness and number of competing publishing nodes.

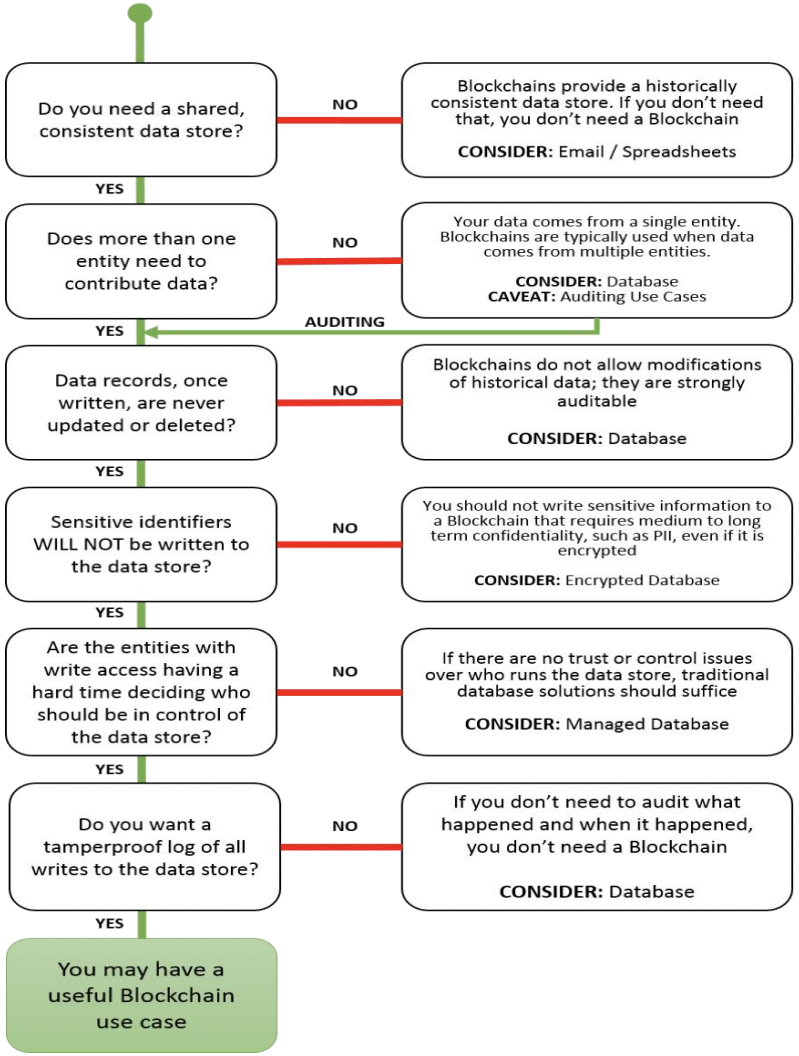
A major part of agreeing on the state of the blockchain network (coming to consensus) is resolving conflicting data.

- node_A creates block_n(A)with transactions #1, 2 and 3. node_A distributes it to some nodes.
- node_B creates block_n(B)with transactions #1, 2 and 4. node_B distributes it to some nodes.

Block B becomes the official blockchain (longer blockchain)

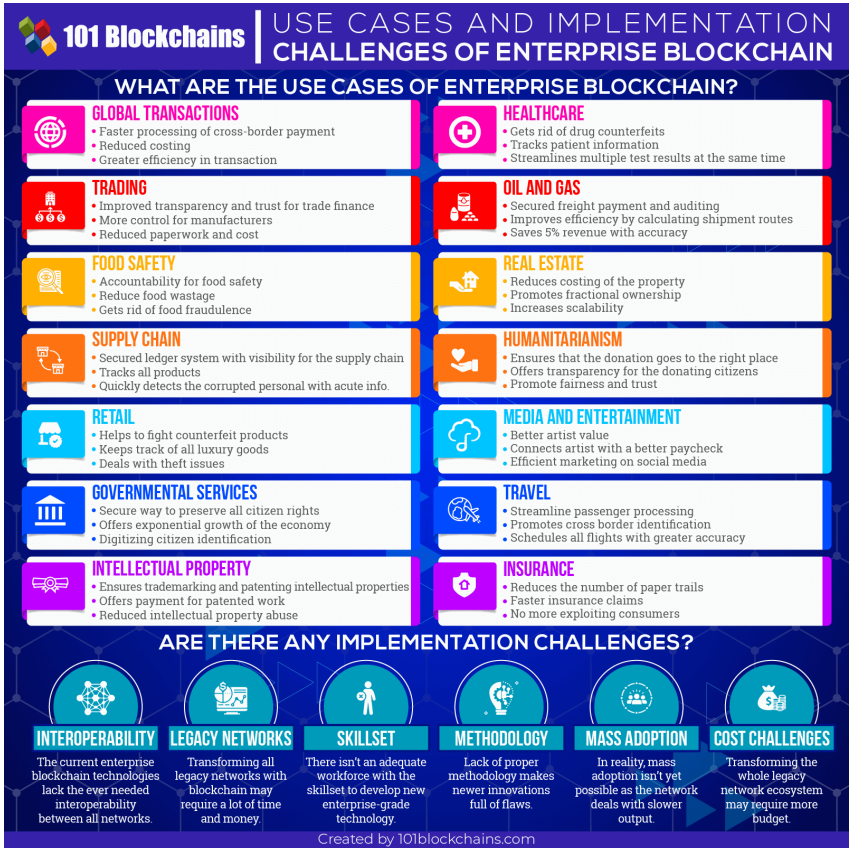


When to use which storage? (Centralized or Distributed?)



DHS Science & Technology Directorate Flowchart

Use Cases of Enterprise Blockchain



Usage of

Industry Gross Value Added (Billions USD)	 **AI**	 **IoT**	 **Blockchain**	 **AR & VR**
Real Estate ($2,462)	Machine and deep learning are allowing firms to build comprehensive property valuation and suggestion models	IoT connected buildings will provide data/information that can influence the economics and value of commercial real estate transactions	Blockchain based smart contracts can streamline property transactions by removing 3rd parties and enabling self executing actions when conditions are met	VR is allowing builders and agents to create virtual property tours for buyers, some of which are on developments that have not yet even broken ground
Health Care ($1,369)	Cognitive systems are taking clinical notes/reports, patient files, external research/data, etc. and generating potential treatment options for doctors to explore further	Wearable sensors that continuously track vitals and update electronic health records will impact home healthcare by giving doctors the ability to remotely monitor patients	Universal health records can be established by aggregating and placing a persons health history onto a blockchain ledger for any HC provider to access and update	VR is advancing medical education by creating immersive virtual simulations from high risk situations to surgical processes at an anatomical level
Finance & Insurance ($1,355)	AI powered insurance chatbots are able to recreate the experience of messaging with an agent to deliver tailored recommendations	Connected sensors allows insurers to collect enough data to offer individualized rates termed usage based insurance, which adapt to a persons real-world behaviors	Initial coin offerings being used to crowdfund early stage projects in cryptocurrency/blockchain industries by releasing their own tokens in exchange for Bitcoin	Holographic workstations presenting immersive real-time financial visualizations may become a standard tool for traders/analysts

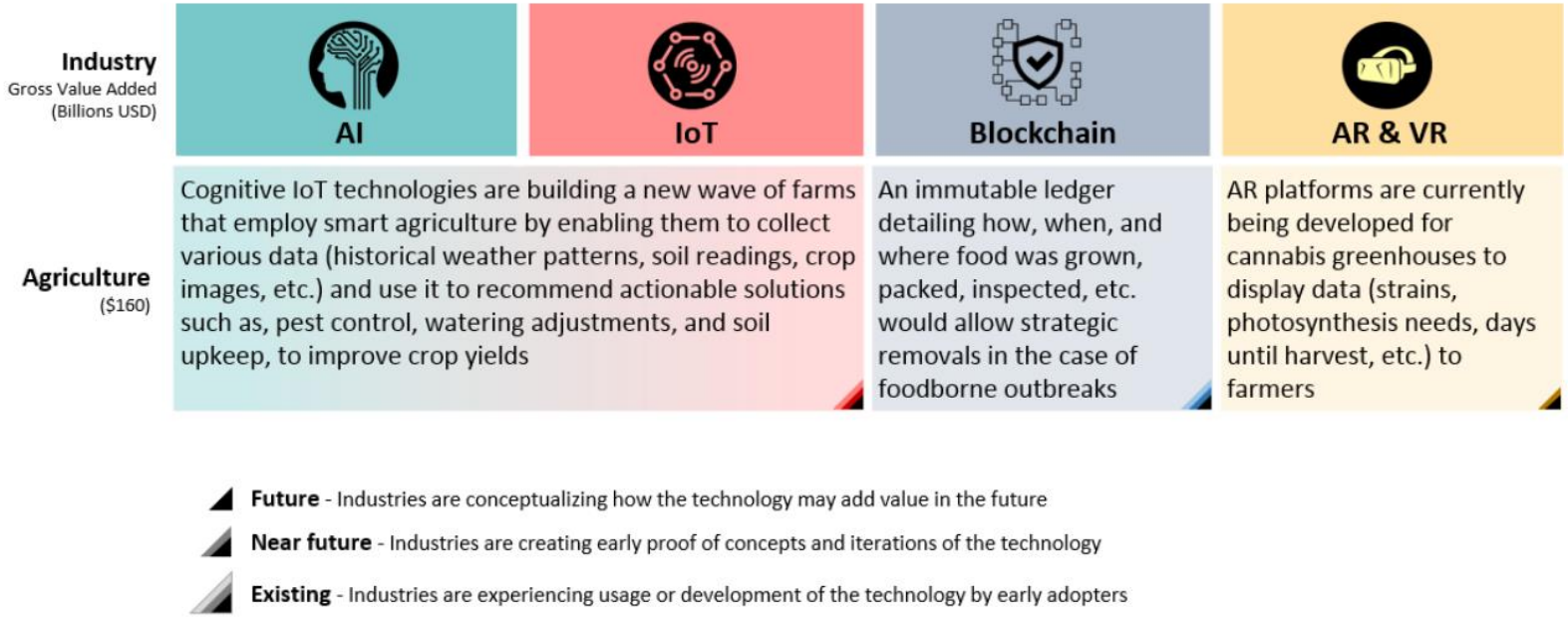
Usage of

Industry Gross Value Added (Billions USD)	AI	IoT	Blockchain	AR & VR
Retail ($1,087)	AI is mastering the art of selling for online retailers by personalizing consumer recommendations based on their digital footprint of behaviors, profile data, etc.	IoT location technologies could enhance retail experiences by sending instant promotions, reviews, or inventories on items as customers move through the aisles	Blockchain will legitimatize transparency of retail supply chains, as raw material and manufacturing sourcing can be recorded to its immutable ledger	AR can enhance the way we shop by displaying and/or filtering info such as, price, promotions, reviews, ratings, etc. to AR devices as customers browse a store
Transport ($503)	Autonomous vehicles will fill our streets over the next decade and bring about packs of driverless long haul trucks called "platoons", which follow a single human driven vehicle through the combination of machine learning and IoT connected sensors		A universally accepted blockchain authenticated ID paired with biometric devices may create a faster and more satisfying experience for travellers	AR is increasing efficiencies in transportation supply chains by creating logistical solutions such as, displaying visuals to aid the warehouse picking process
Pharma & Chemical ($387)	Big Pharma has the potential to test how likely specific combinations of molecules are to make a useful drug by applying machine learning to predict how they will behave	Smart pills (ingestible sensors) are being used to record physiological metrics, spot irregularities, and diagnose illnesses at earlier stages	Blockchain can help combat the $75 billion counterfeit medication market by tracking production, which will build a secure and transparent supply chain ledger	VR is being used to increase worker health and safety within manufacturing environments by recreating simulated emergency experiences such as, chemical spills

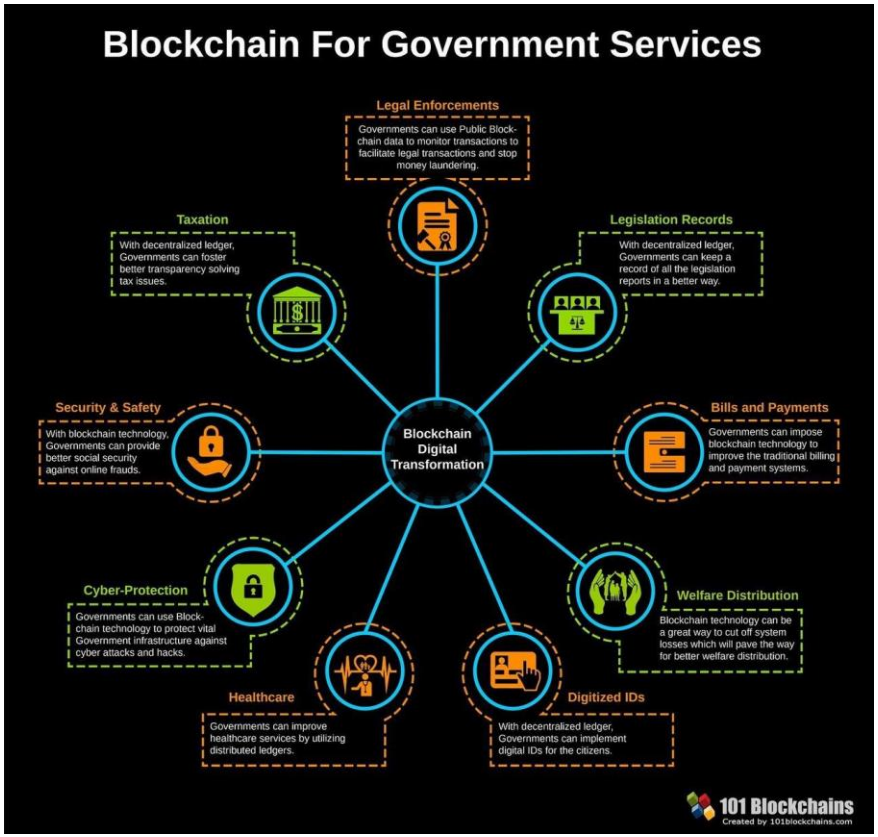
Usage of

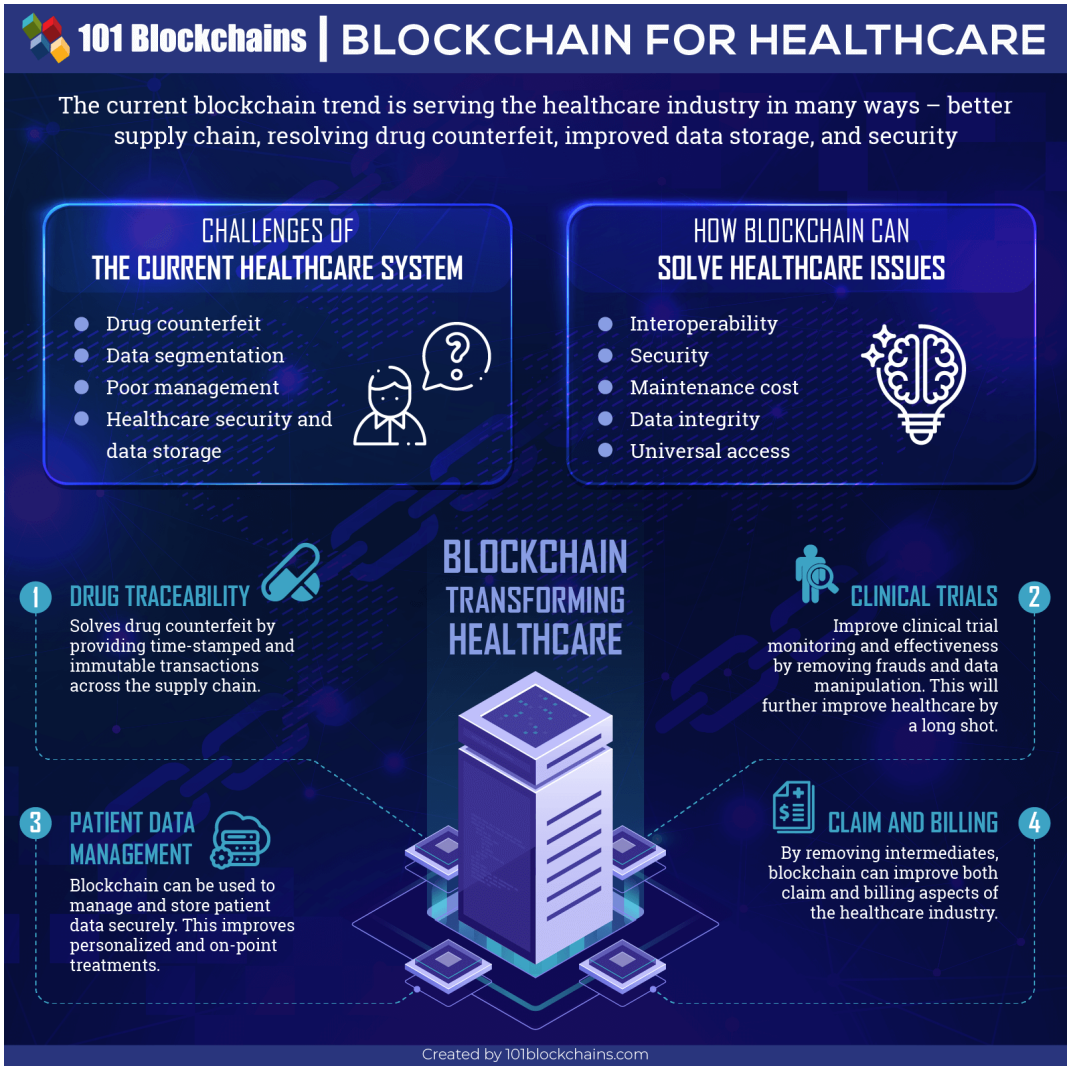
Industry Gross Value Added (Billions USD)	AI	IoT	Blockchain	AR & VR
Aerospace & Defense ($307)	AI is powering swarms of autonomous micro-drones to advance the stealth tracking and searching capabilities of the defense department	Networks of sensors such as, Lockheed Martin's ALIS, are being embedded on aircraft to detect performance and communicate maintenance needs to ground repair staff; systems like ALIS can use blockchain technology to create a single united ledger that will form a digital copy from every part to mechanic that touches the plane		Troops are being deployed with helmets capable of displaying real-time information through AR, which create advantages in the air and on the battlefield
Utilities & Energy ($288)	Networks of connected sensors throughout appliances and devices can use machine learning to gauge, learn, and anticipate user behaviors and autonomously control a home or buildings energy for optimized consumption, this should ultimately help balance the supply and demand of large-scale energy grids		Cryptocurrencies could reduce disputed energy transactions by quickly processing payments on a transparent ledger with no 3rd party validation required	Experiments using AR headsets to provide field workers with instant information and visuals are currently underway with hopes to improve operational efficiencies
Education ($207)	AI is empowering intelligent online tutoring systems, which may evolve into "lifelong learning companions" that can gather data and support learners as they grow and develop their knowledge	Connected wearable's may help teachers adapt curricula by providing student data such as, brain activity while testing various teaching styles to new classes	Blockchain has the power to create a centralized ledger of coursework and open the availability of accredited higher education to developing nations by validating the completion MOOC certifications	AR/VR will be used to onboard new employees more effectively by immersing them in virtual environments featuring both educational and interactive problem solving challenges

Usage of

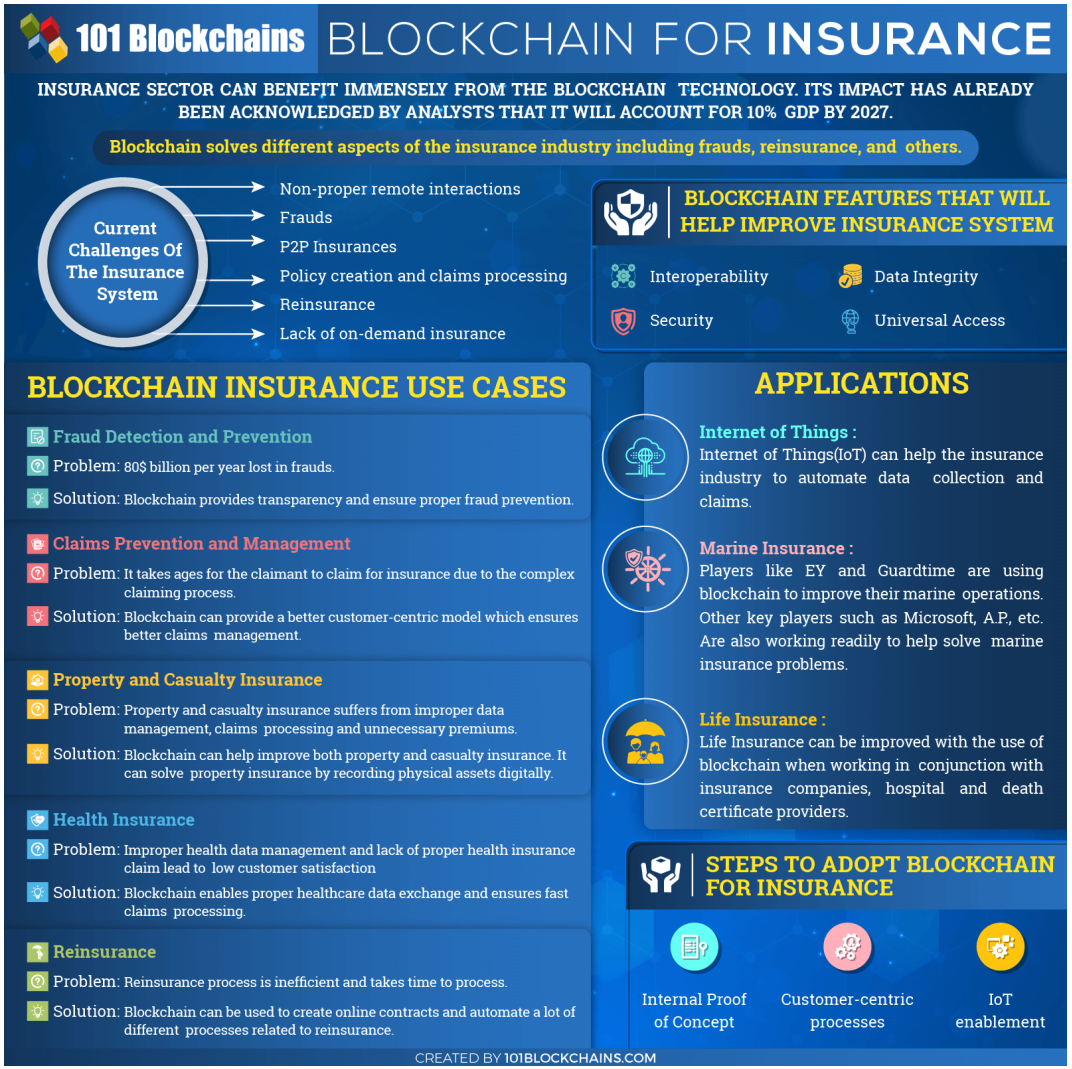


Blockchain example





Blockchain Transforming Healthcare



Blockchain Insurance Use Cases