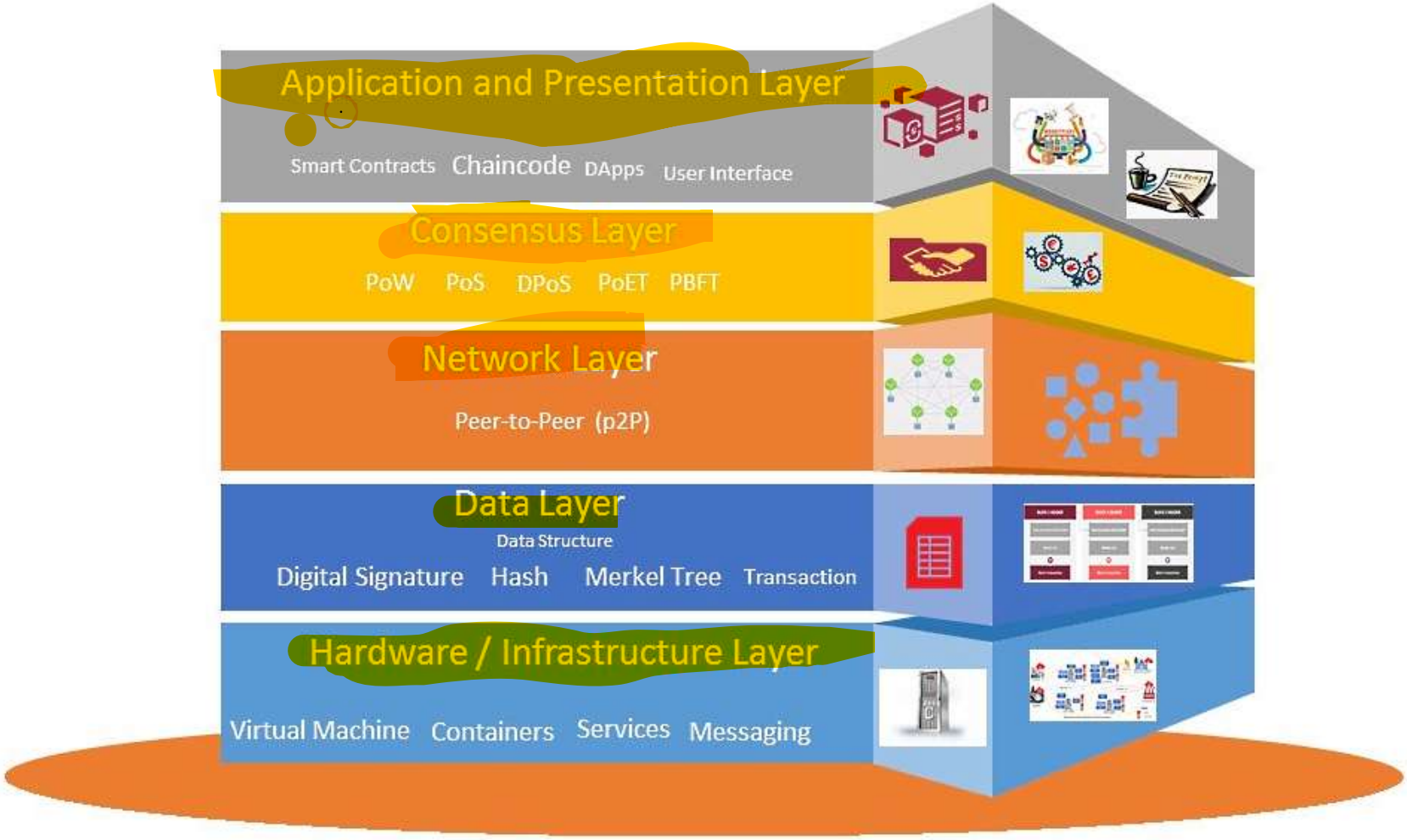
Lect 13-15_Understanding the Layers of Blockchain Technology

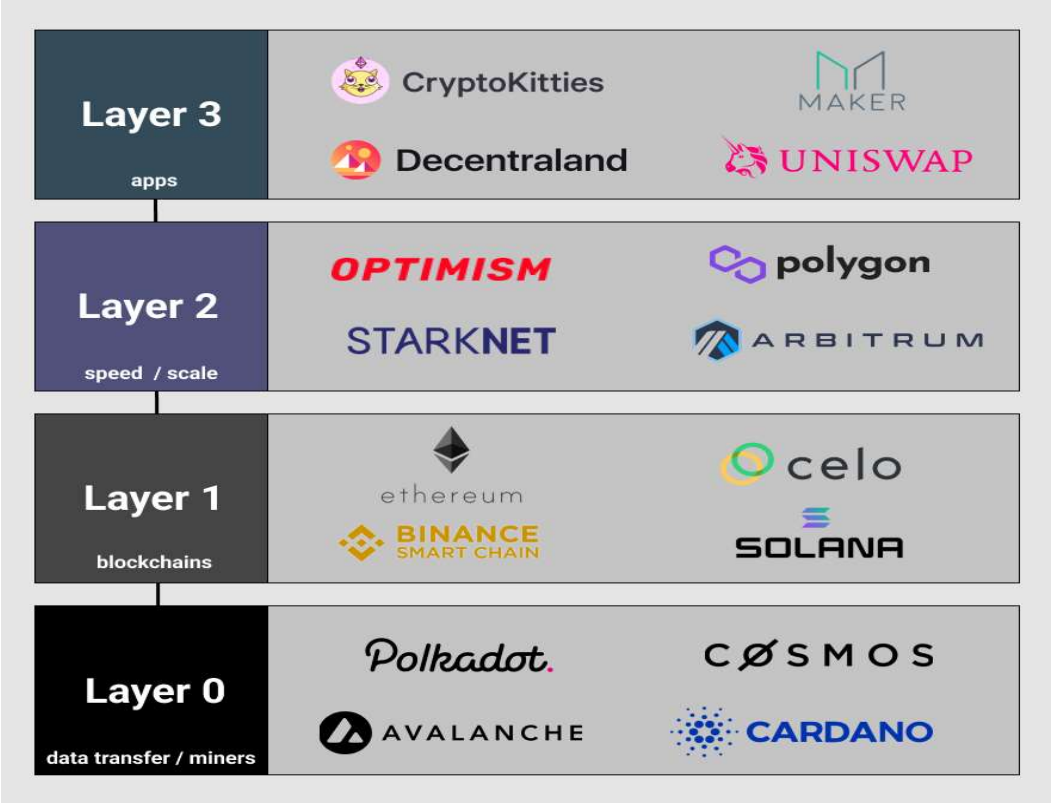
The layered architecture of blockchain is categorized into five layers



There are five layers of blockchain technology:

- According to some blockchain professionals, there are five layers of blockchain technology:
- Infrastructure or hardware layer
- Data layer
- Network layer
- Consensus layer
- Application and presentation layers

However, blockchain technology layers can also be categorized as:



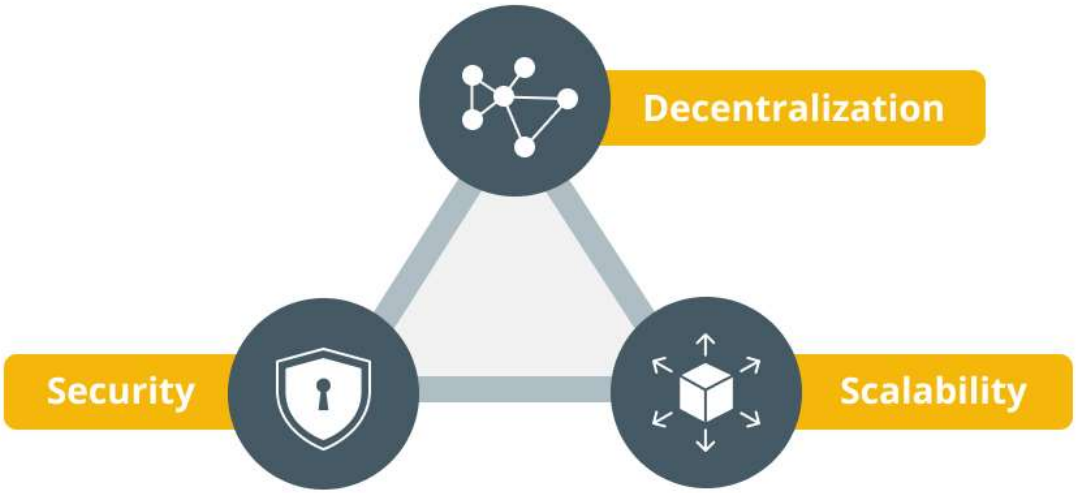
Layer 0

- This is where the internet, hardware, and connections exist that allow layer 1s like Bitcoin to run smoothly. Layer 0s are allowing several things to happen:
- **1) Allow blockchains to interact with each other**
- **2) Faster and cheaper transactions**
- **3) Infrastructure for developers**

Layer 1

- Layer 1s are blockchains (Bitcoin and Ethereum) that process and finalize transactions on their own blockchain. This is where things like consensus (PoW, PoS) and all the technical details like block time and dispute resolution take place.
- The most important three aspects of blockchains are conquering the blockchain trilemma: decentralization, security, and scalability.

The blockchain trilemma



cointelegraph.com

source: ***Seba***

Blockchain trilemma's dynamics

- Before delving into the trilemma's dynamics, let's define scalability, security and decentralization in general terms:
  - The blockchain's scalability refers to its ability to handle a higher volume of transactions.
  - Security refers to the ability to secure data on the blockchain from various types of assaults and the blockchain's defense against double-spending.
  - Decentralization is a type of network redundancy that ensures that the network is not controlled by fewer entities.

Layer 2

- Layer 2s are third-party integrations used in conjunction with layer ones to increase scalability and transactions per second (system throughput).

Layer 3

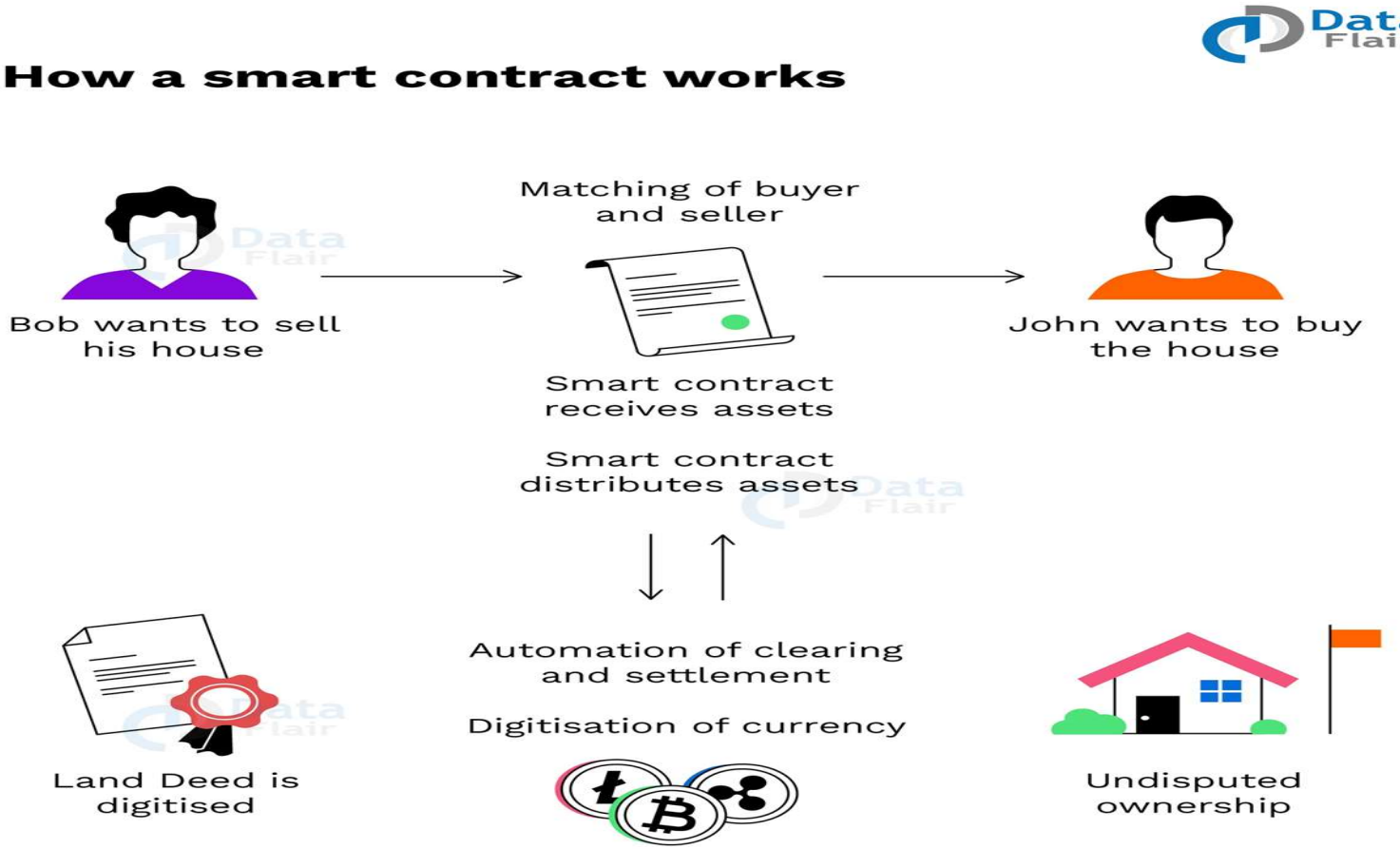
- Layer 3 is the application layer. This is the UI that we as consumers actually interact with.

Smart Contracts and How smart contracts work

- A smart contract is a computer code that can be built into the blockchain to facilitate, verify, or negotiate a contract agreement.
- Smart contracts operate under a set of conditions to which users agree. When those conditions are met, the terms of the agreement are automatically carried out.
- Smart contracts work by following simple "if/when…then…" statements that are written into code on a blockchain.
- A network of computers executes the actions when predetermined conditions have been met and verified.
- These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed.

Traditional Contract and Smart Contract

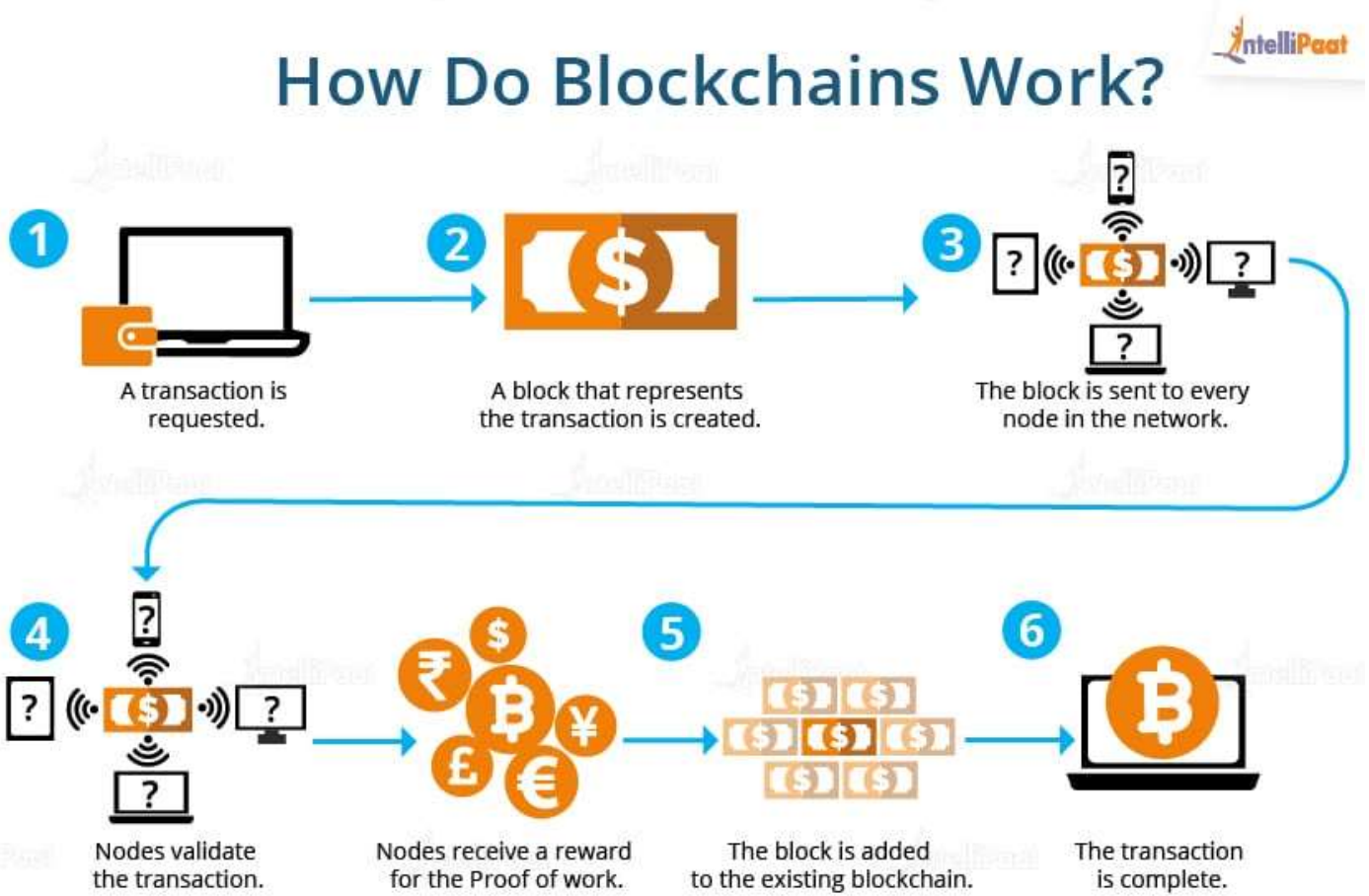
Smart Contract Work



Transaction in blockchain

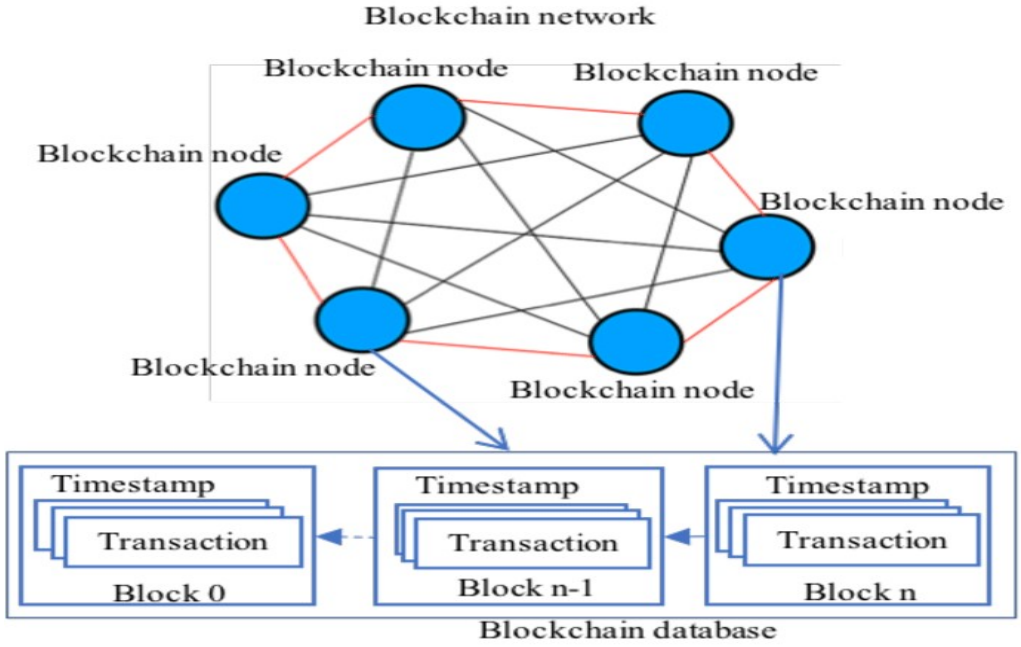
- For a public blockchain, **the decision to add a transaction to the chain is made by consensus**.
- This means that the majority of "nodes" (or computers in the network) must agree that the transaction is valid.
- The people who own the computers in the network are incentivised to verify transactions through rewards.

Blockchain


How Do Blockchains Work?
IntelliPaat
1
A transaction is requested.
2
A block that represents the transaction is created.
3
The block is sent to every node in the network.
4
Nodes validate the transaction.
Nodes receive a reward for the Proof of work.
5
The block is added to the existing blockchain.
6
The transaction is complete.

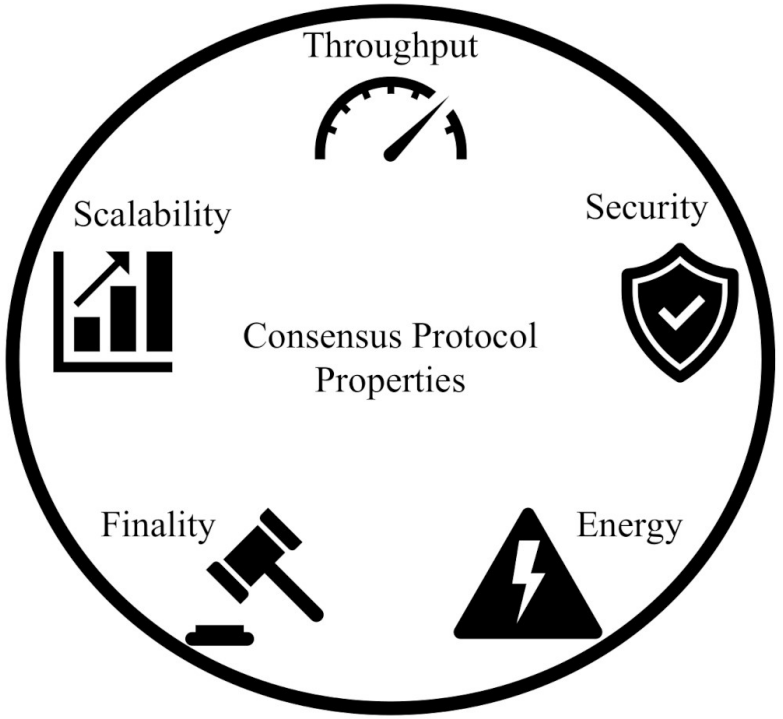
Blockchain Networks

- A blockchain network is **a technical infrastructure that provides ledger and smart contract (chaincode) services to applications**.

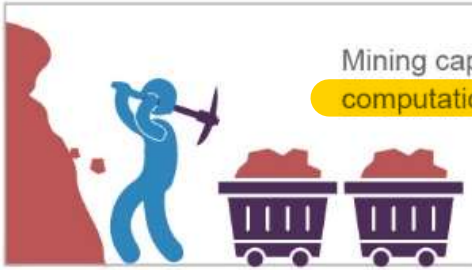


Consensus algorithm

- A consensus algorithm is **a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger**.



Proof of Work VS Proof of Stake



Mining capacity depends on computational power

Validating capacity depends on the stake in the network

Miners receive block rewards to solve a cryptographic puzzle

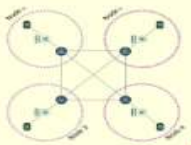
Validators do not receive a block reward, instead, they collect transaction fees as reward

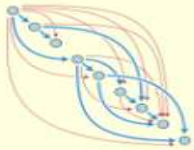
Hackers would need to have a computer powerful than 51% of the network to add a malicious block, leading to 51% attack

Hacker would need to own 51% of all the cryptocurrency on the network, which is practically impossible and therefore, making 51% attacks impossible.

masterthecrypto

Comparison of Consensus Algorithms





	Proof-of-Work (POW)	Proof-of-Stake (POS)	Delegated Proof-of-Stake (DPOS)	Byzantine Fault Tolerance	Directed Acyclic Graphs (DAG)
Energy Consumption	High	Low	Very Low	Very Low	Very Low
Transaction Per Second	7	30 - 173	2.5 - 2,500	100 - 2,500	180 - 7,000
Transaction Fees	High	Low	Low	Very Low	None
Structure	Decentralized	Decentralized	Centralized	Decentralized	Decentralized
Example	Bitcoin	Dash	Bitshares	Stellar	IOTA

Byzantine Fault-Tolerant (BFT Protocols)

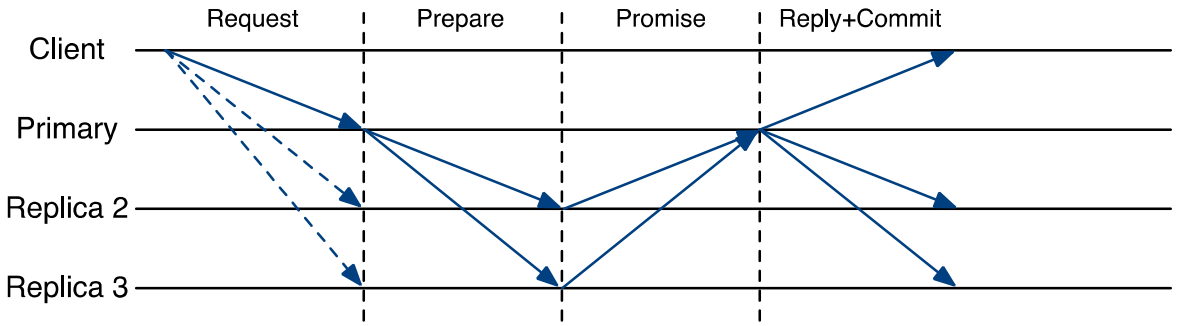
- Traditionally important
  - Powerful: Byzantine/arbitrary failures & attacks
  - Systems, distributed systems, theory, crypto, security, …
- Recently gain prominence
  - Real threats to real systems
  - Blockchains
  - Mission-critical systems (SpaceX)
  - …

State Machine Replication

Paxos

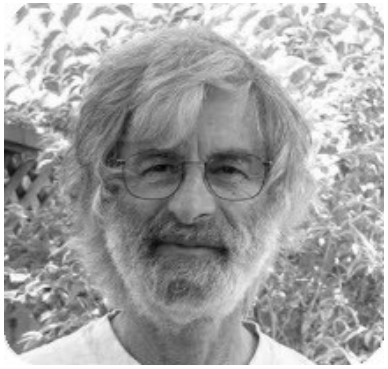
[Lamport, ACM TOCS 1998]; going back to 1989

[Lamport. Paxos made simple. ACM SIGACT News 2001]



"For fundamental contributions to the theory and practice of distributed and concurrent systems, notably the invention of concepts such as causality and logical clocks, safety and liveness, replicated state machines, and sequential consistency."

Turing Award 2013



Leslie Lamport

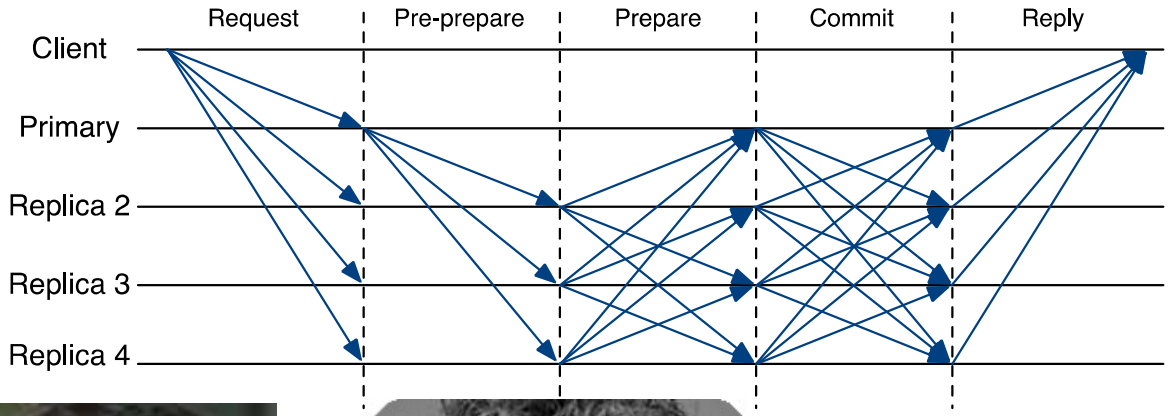
- For fundamental contributions to the theory and practice of distributed and concurrent systems, notably the invention of concepts such as causality and logical clocks, safety and liveness, replicated state machines, and sequential consistency.

State Machine Replication

PBFT

- 3*f*+1 replicas to tolerate *f* Byzantine failures

[Castro and Liskov, OSDI 1999]



"For contributions to practical and theoretical foundations of programming language and system design, especially related to data abstraction, fault tolerance, and distributed computing."

Turing Award 2008

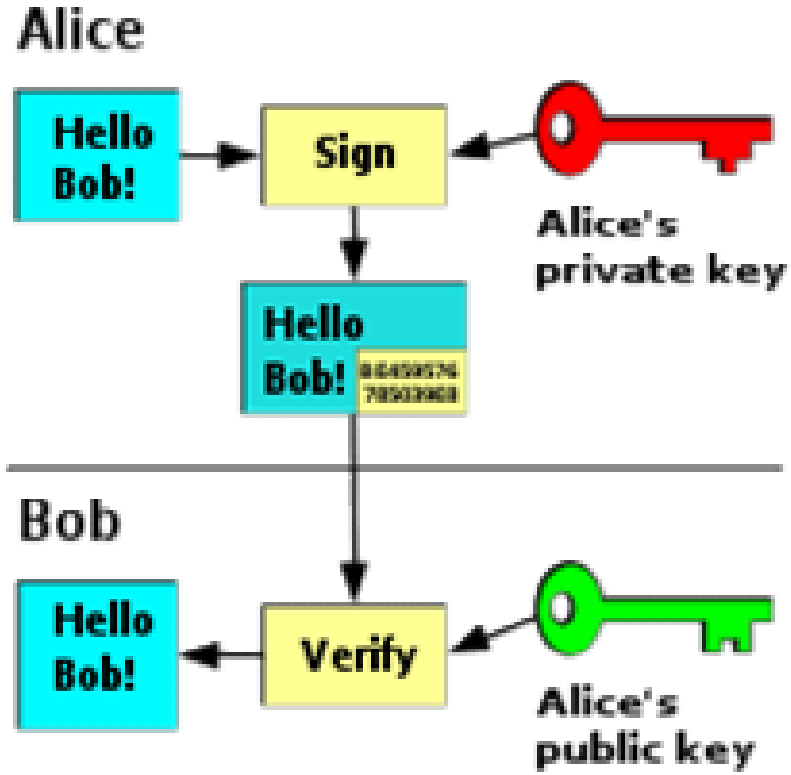
Barbara Liskov

- For contributions to practical and theoretical foundations of programming language and system design, especially related to data abstraction, fault tolerance, and distributed computing.

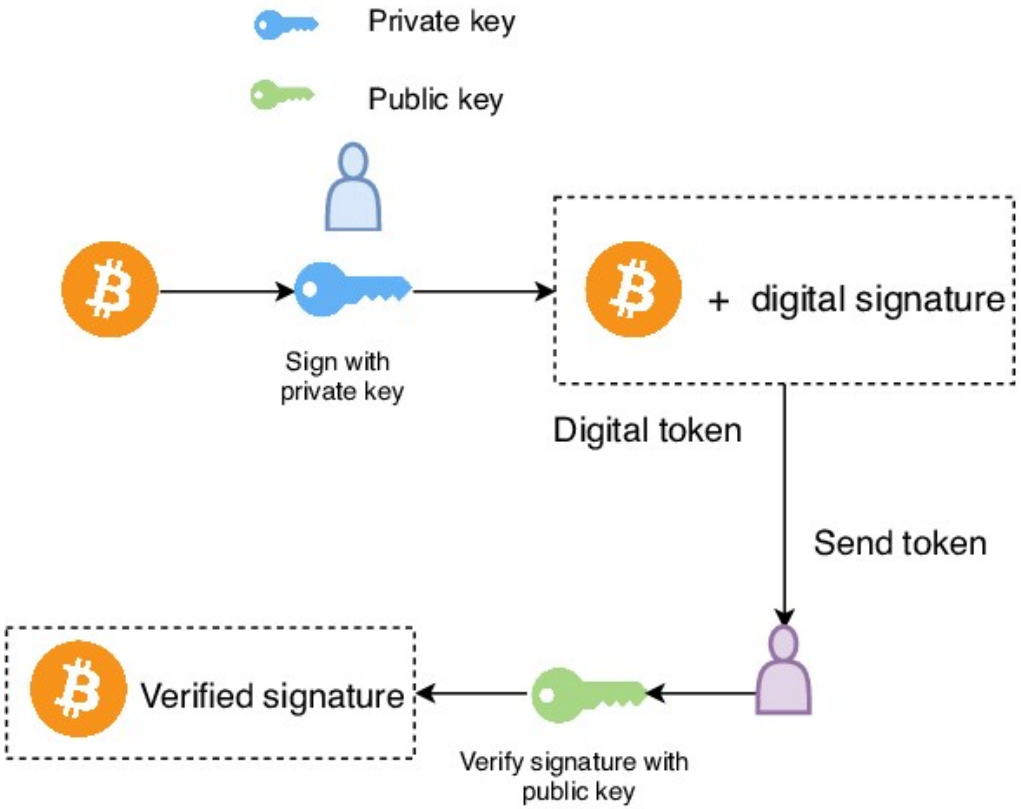
Digital signature

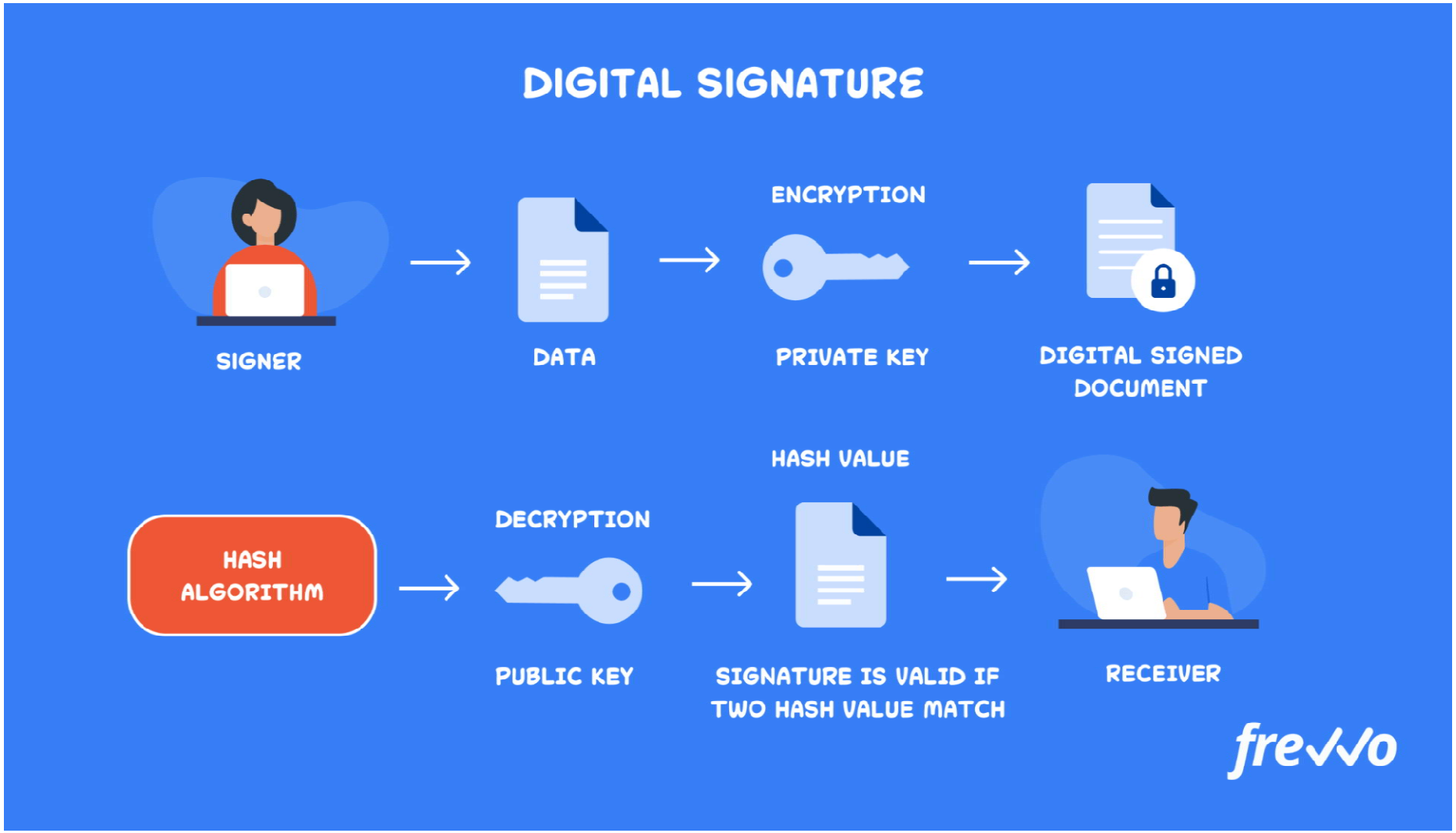
- A digital signature is **a cryptographic output used to verify the authenticity of data**.
- A digital signature algorithm allows for two distinct operations: a signing operation, which uses a signing key to produce a signature over raw data.

Digital Signature

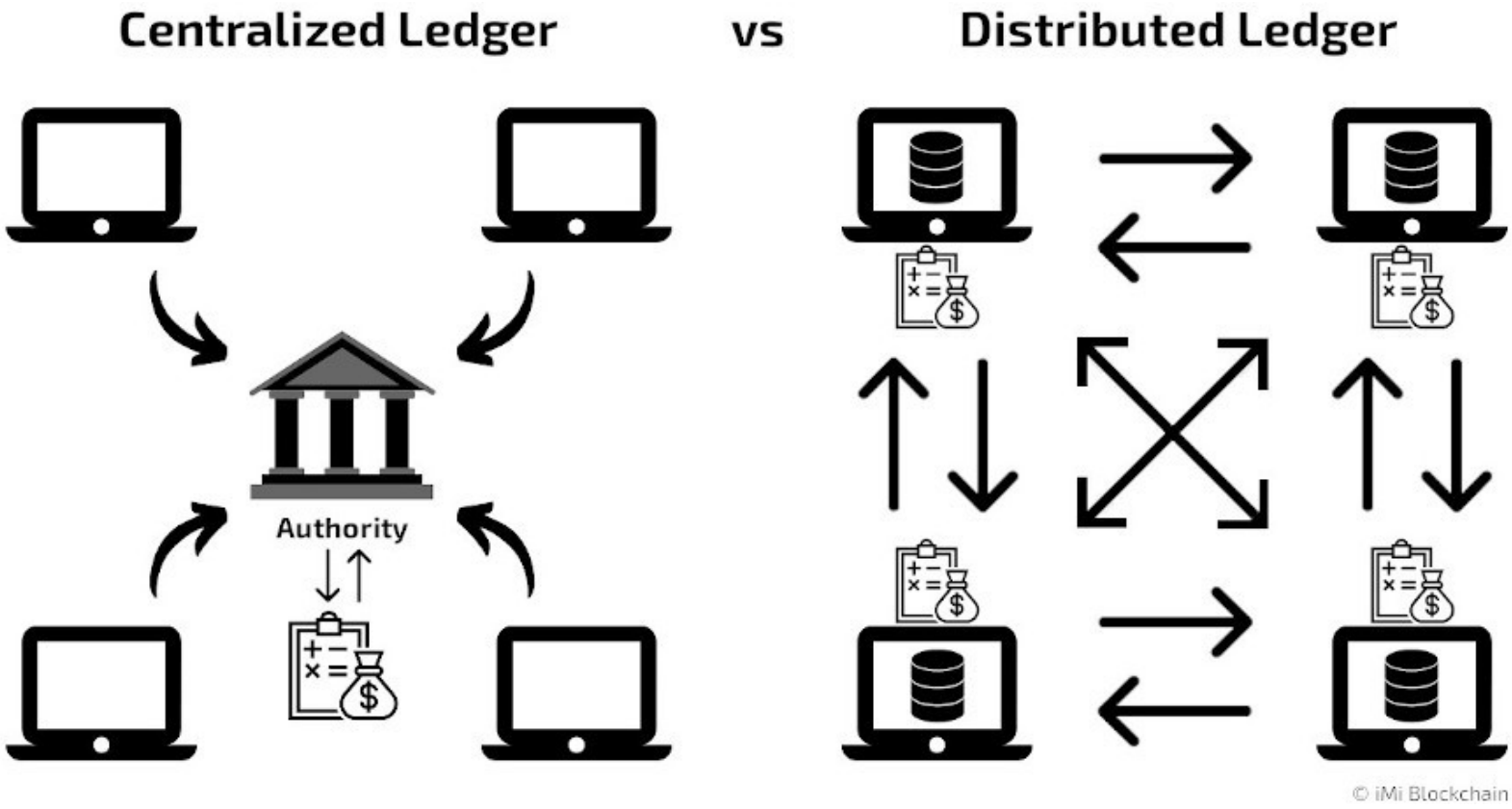


Simplified digitally signed transaction on blockchain.




DIGITAL SIGNATURE
SIGNER
DATA
ENCRYPTION
PRIVATE KEY
DIGITAL SIGNED DOCUMENT
HASH ALGORITHM
DECRYPTION
PUBLIC KEY
HASH VALUE
SIGNATURE IS VALID IF TWO HASH VALUE MATCH
RECEIVER
frevvo

distributed ledger technology blockchain



Blockchain Applications

- Money transfers. The original concept behind the invention of blockchain technology is still a great application. ...
- Financial exchanges. ...
- Lending. ...
- Insurance. ...
- Real estate. ...
- Secure personal information. ...
- Voting. ...
- Government benefits.

Where Might Blockchain Use Cryptography?

Initiation and Broadcasting of Transaction	• *Digital Signatures* • *Private/Public Keys*
Validation of Transaction	• *Proof of Work and certain alternatives*
Chaining Blocks	• *Hash Function*

30.33

॥ त्वं ज्ञानमयो विज्ञानमयोऽसि ॥

Thank you!