Blockchain and Consensus

Contents

- Introduction to Blockchain: Digital Trust, Asset, Transactions, Distributed Ledger Technology, Types of network, Components of blockchain (cryptography, ledgers, consensus, smart contracts). (5 Lectures)
- PKI and Cryptography: Private keys, Public keys, Hashing, Digital Signature. (6 Lectures)
- Consensus: Byzantine Fault, Proof of Work, Proof of Stake. (6 Lectures)

Evaluation Scheme

Components	Weightage	
Minor 1 and Minor 2	20%-30%	
Assignments	20%	
Quizes	20%	
End Sem (Major)	30%-40%	

Digital Trust in Blockchain

- Digital trust is **the confidence users have in the ability of people, technology and processes to create a secure digital world**.
- Digital trust is a kind of user heuristics in blockchain.
- Blockchain users are likely cope with the perceived risk, security, and privacy, and overload by using heuristics that minimize their cognitive effort and time, through the use of cognitive heuristics.
- Digital trust as cognitive heuristics constitute information processing methods to make decisions more quickly and with less effort than more complex methods, and thus they reduce cognitive load during security assessment.

Assets

- Blockchain assets are **a type of digital asset or cryptocurrency**

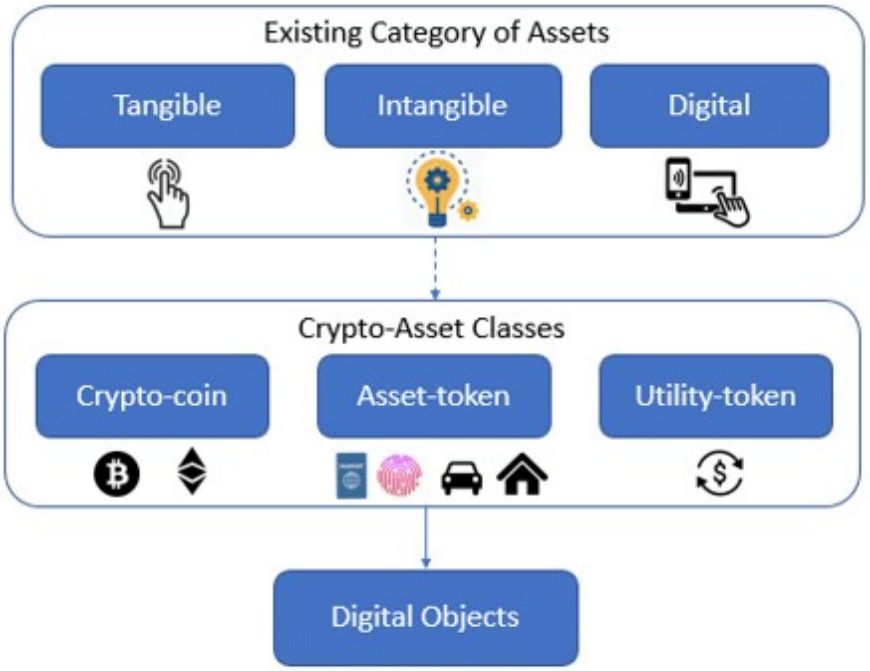
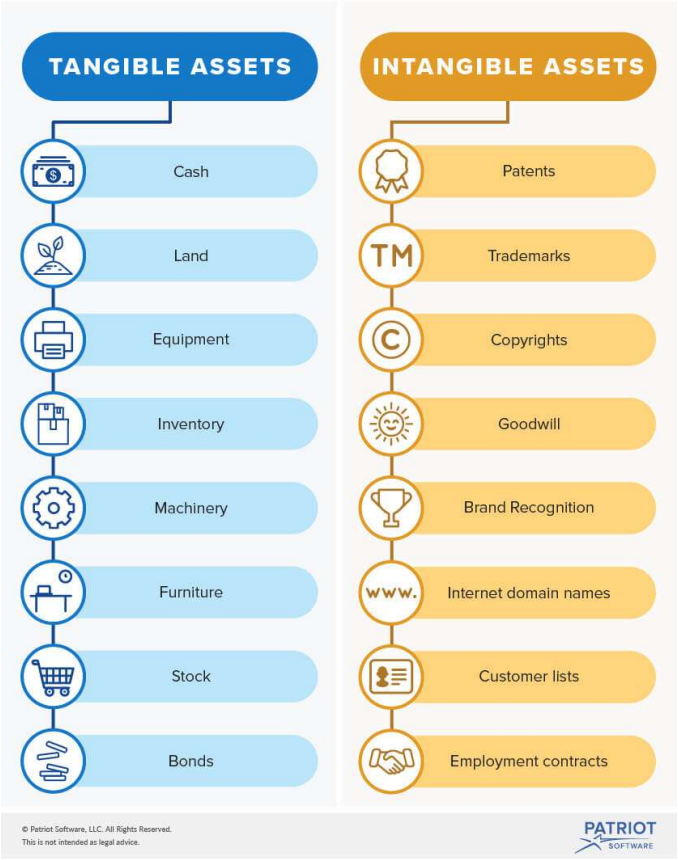


Fig. 1. Blockchain crypto-asset classes

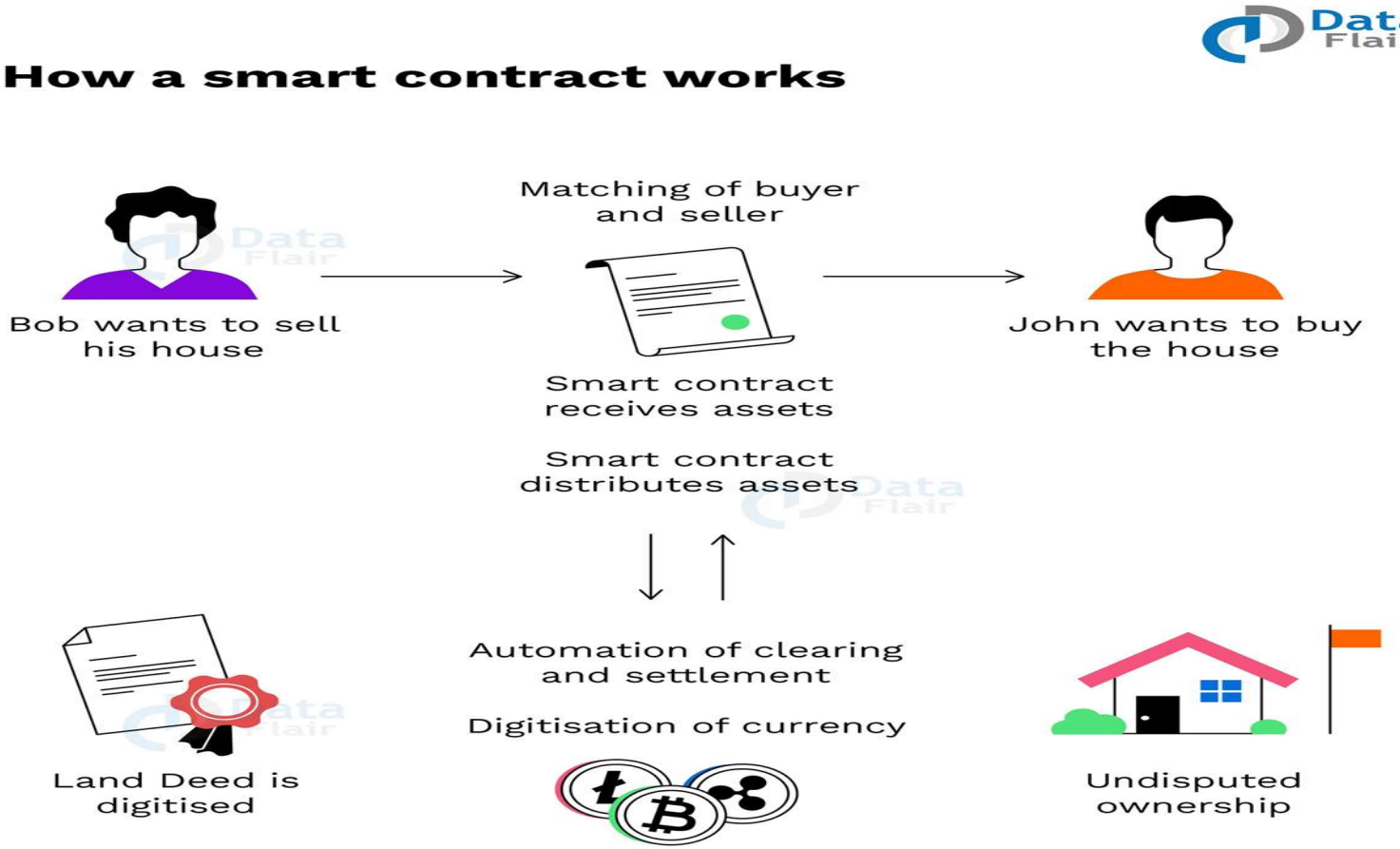


Smart Contracts and How smart contracts work

- 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

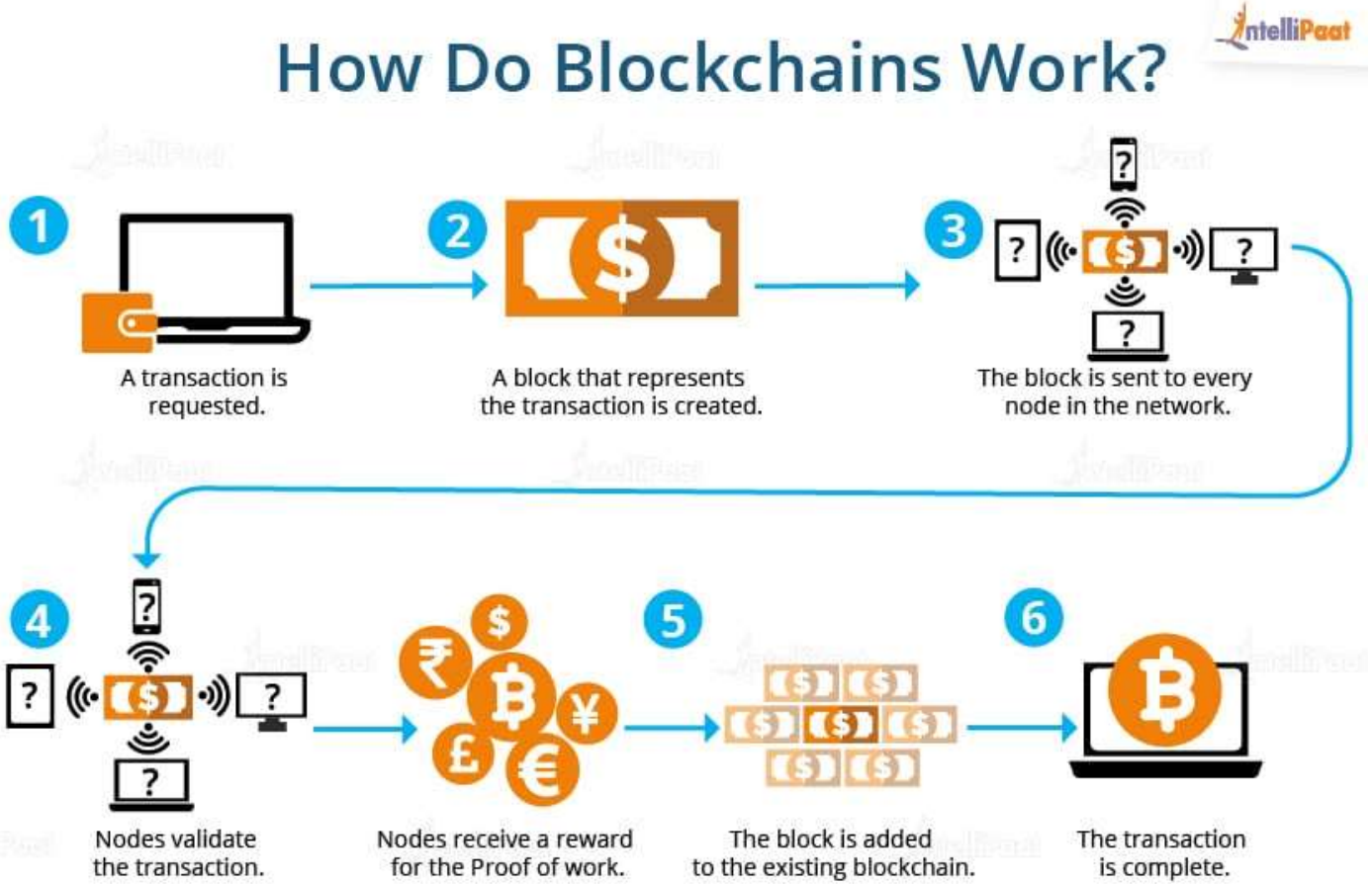
Smart Contract Work



Transaction in blockchain

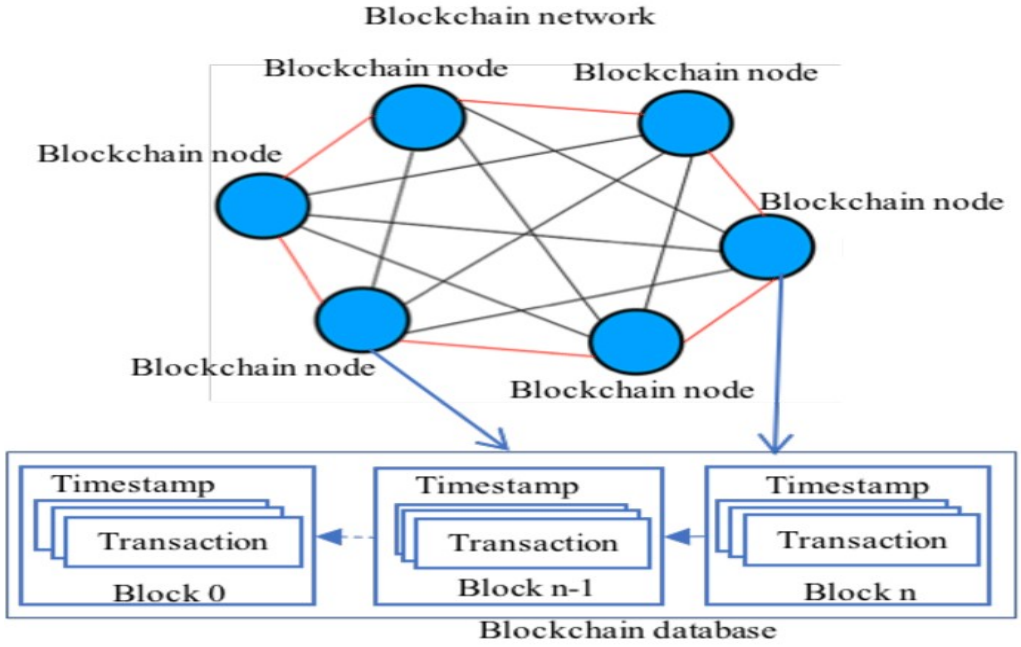
- For a public blockchain, **the decision to add a transaction to the chain is made by consensus**.
- This means that the majority of “nodes” (or computers in the network) must agree that the transaction is valid.
- The people who own the computers in the network are incentivised to verify transactions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

Blockchain

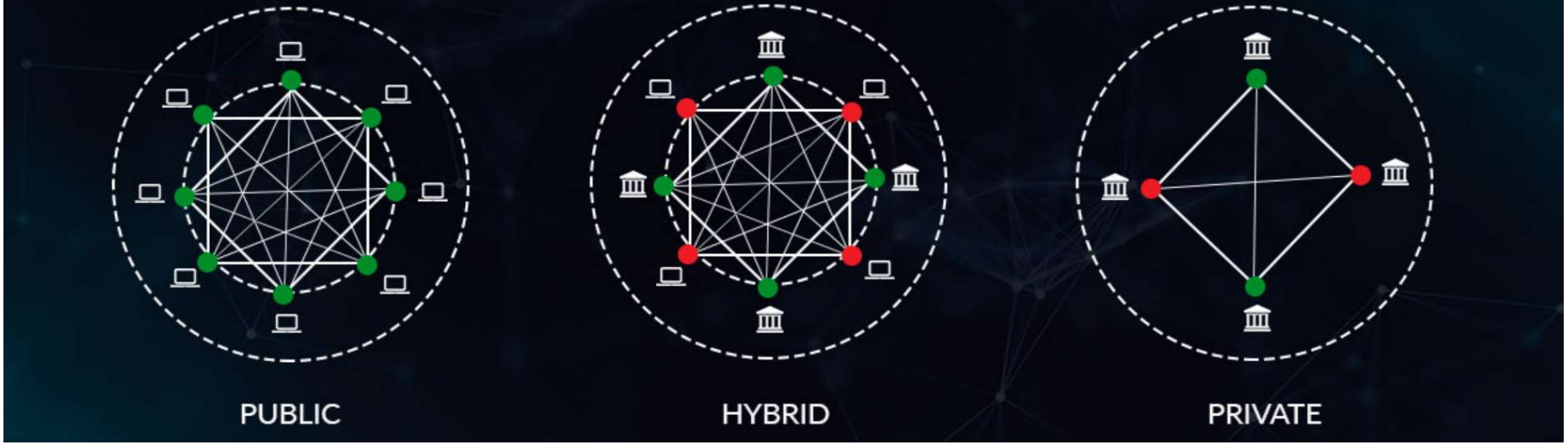

How Do Blockchains Work?
IntelliPaat
1
A transaction is requested.
2
A block that represents the transaction is created.
3
The block is sent to every node in the network.
4
Nodes validate the transaction.
Nodes receive a reward for the Proof of work.
5
The block is added to the existing blockchain.
6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

Blockchain Networks

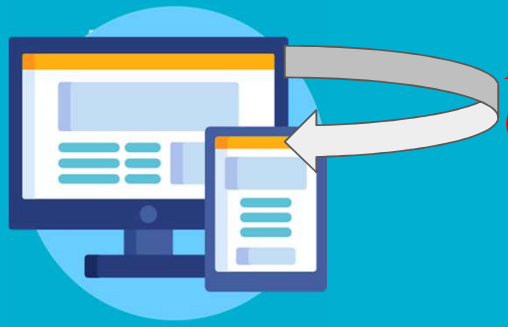
- A blockchain network is **a technical infrastructure that provides ledger and smart contract (chaincode) services to applications.**



Types of Blockchain

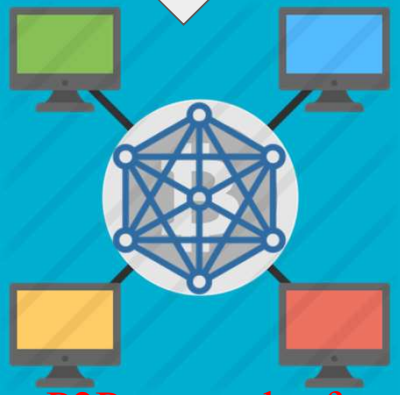


Transaction execution in Blockchain



A Blockchain normal node (e.g., computer or mobile), create transaction

The transaction broadcast to network of all P2P miner nodes



P2P network of miner nodes

Nodes verifies the transaction using public key cryptography

Verified transaction, and linked to other transaction to create new block

New Block

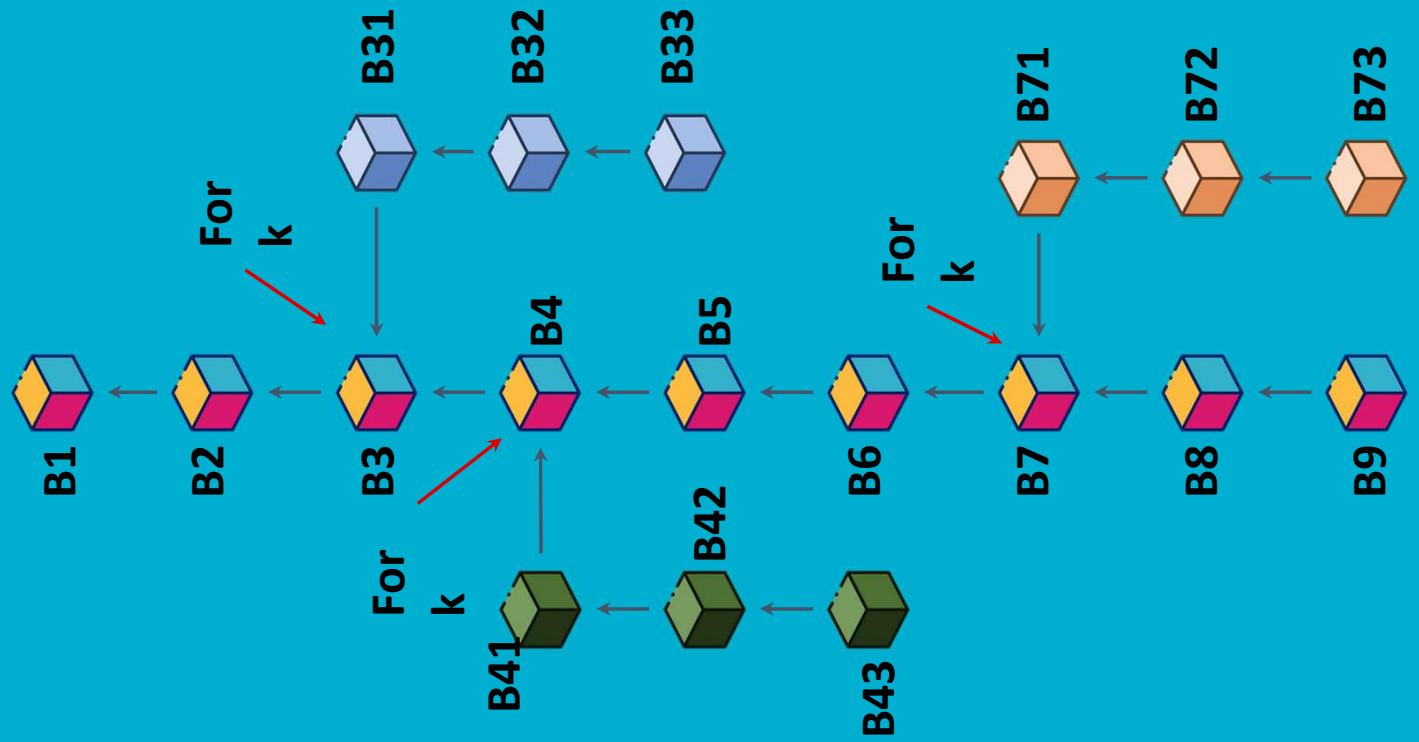
New Block is appended into existing blockchain

New Block

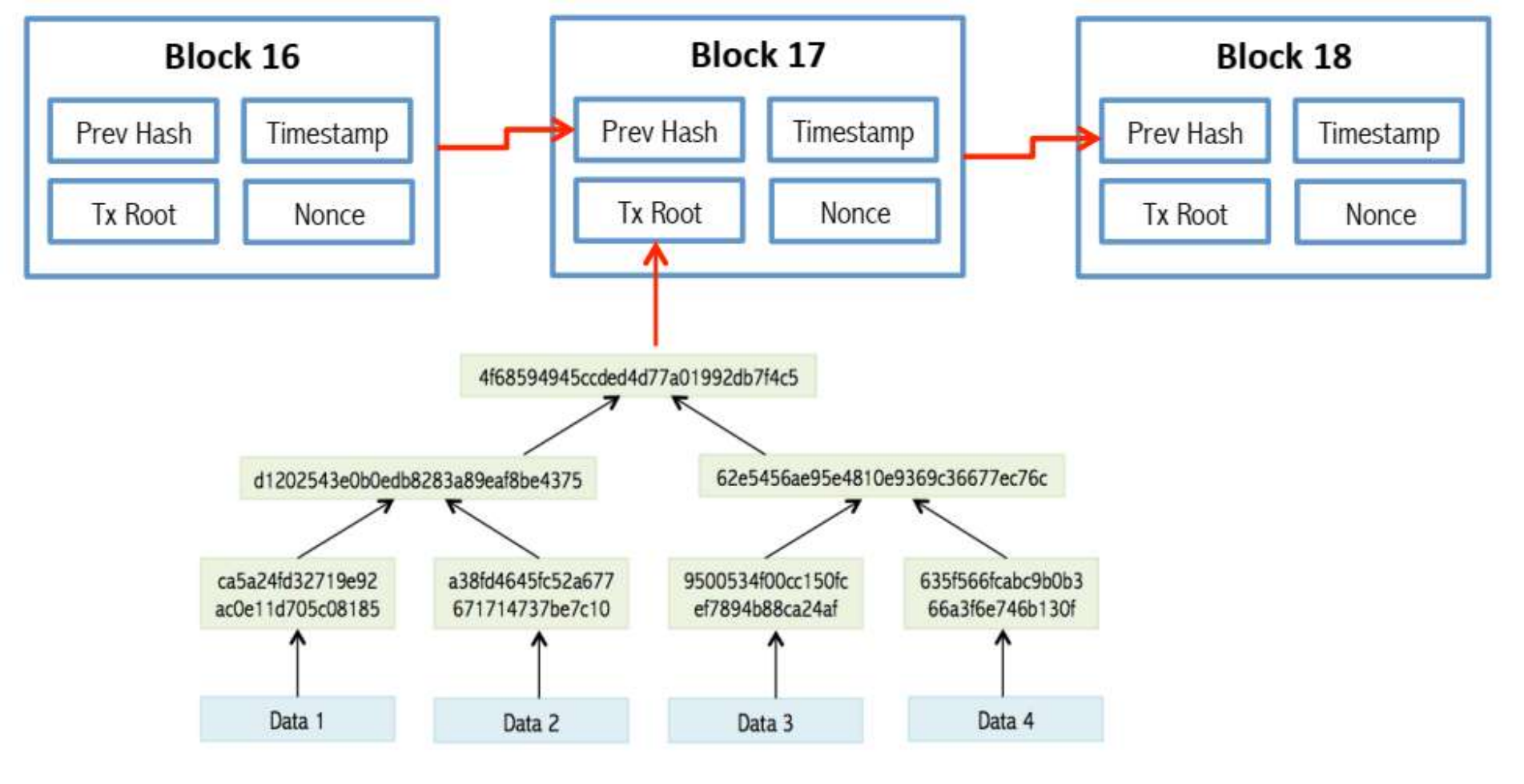
Old Blocks

The Transaction is complete

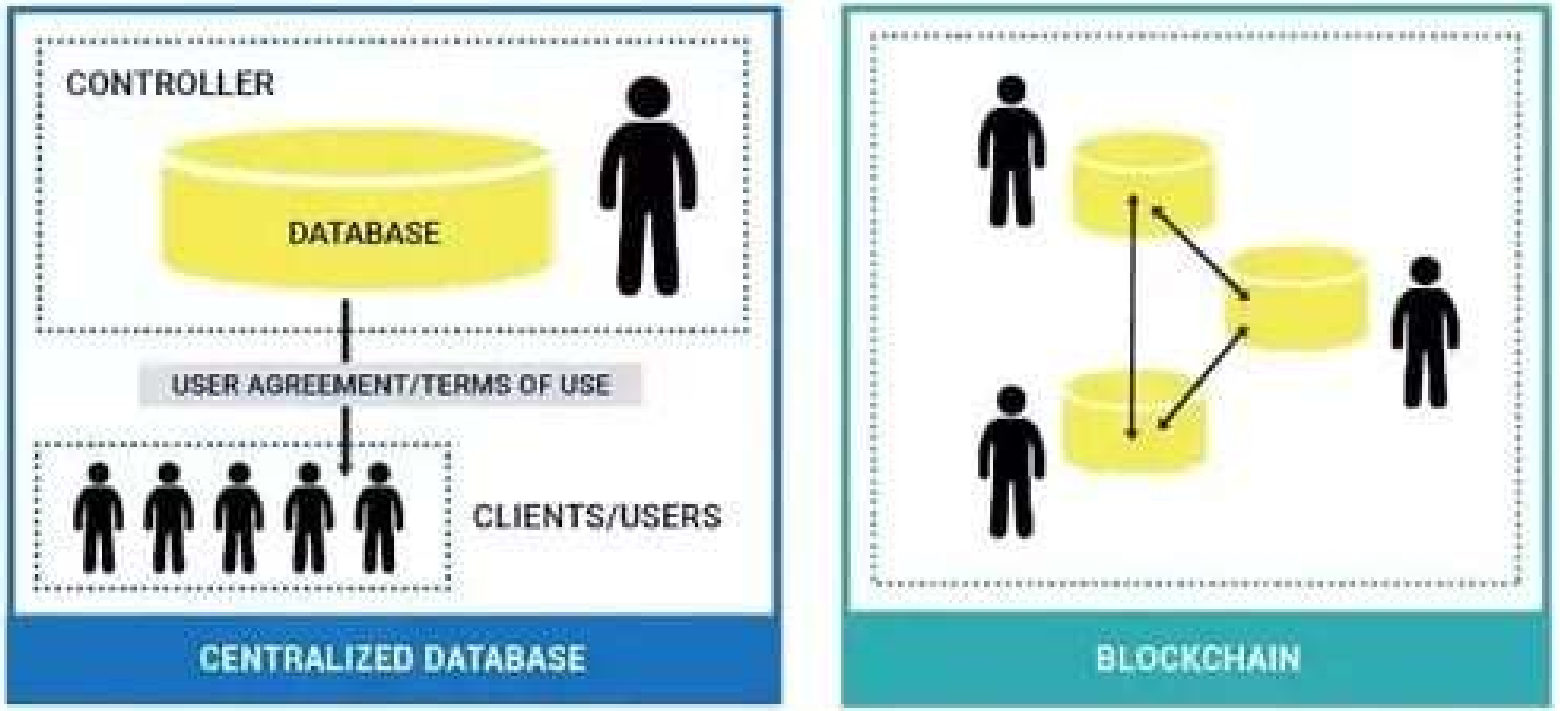
Structure


B1
B2
B3
For k
B31
B32
B33
B4
B5
B6
For k
B71
B72
B73
B7
B8
B9
For k
B41
B42
B43

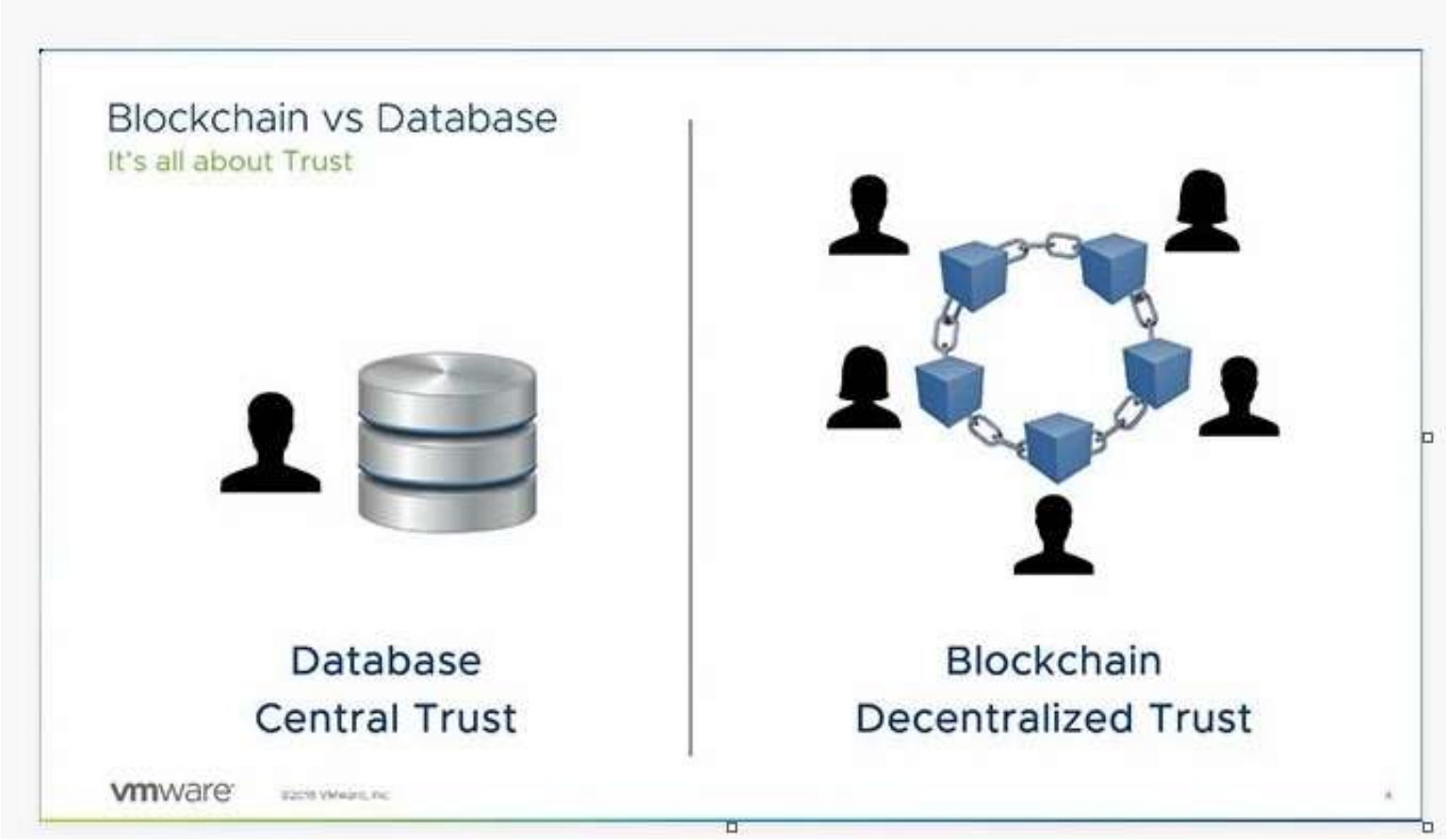
The data structure of the Bitcoin Blockchains



CENTRALIZED DATABASES VS. BLOCKCHAIN

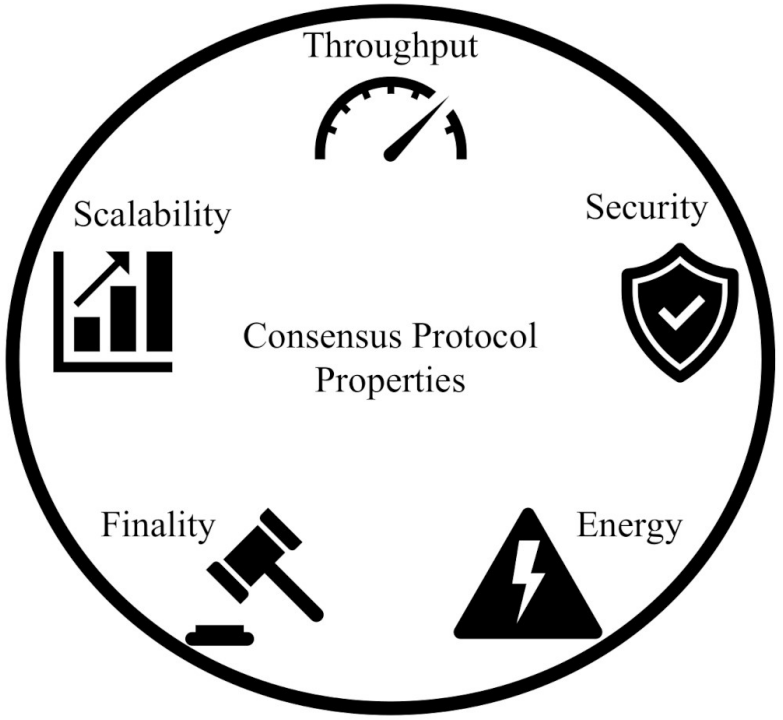


Blockchain Decentralized Trust



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.

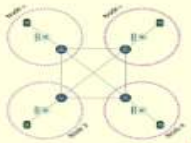
masterthecrypto

Comparison of Consensus Algorithms

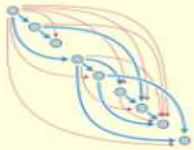
Proof-of-Work (POW)

Proof-of-Stake (POS)

Delegated Proof-of-Stake (DPOS)



Byzantine Fault Tolerance



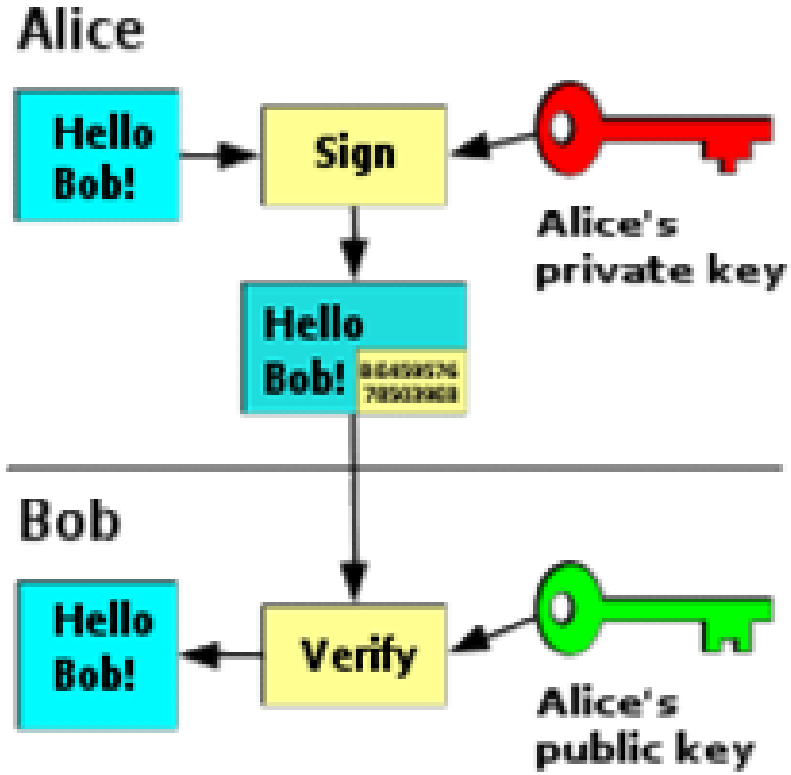
Directed Acyclic Graphs (DAG)

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

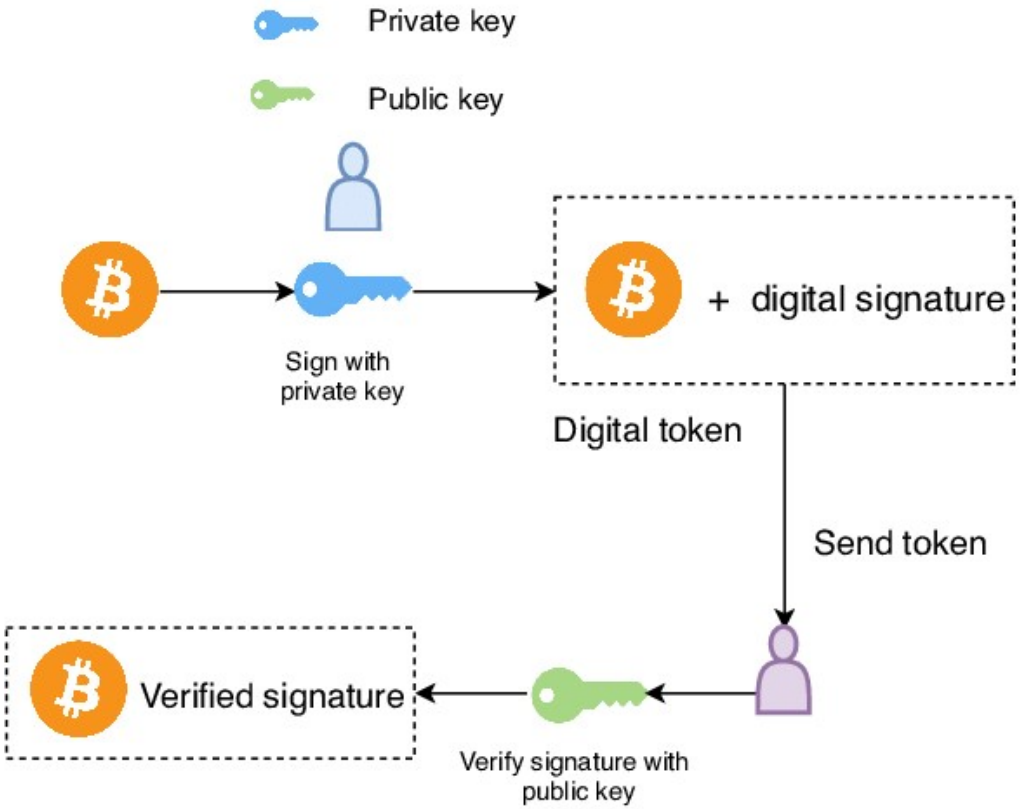
Digital signature

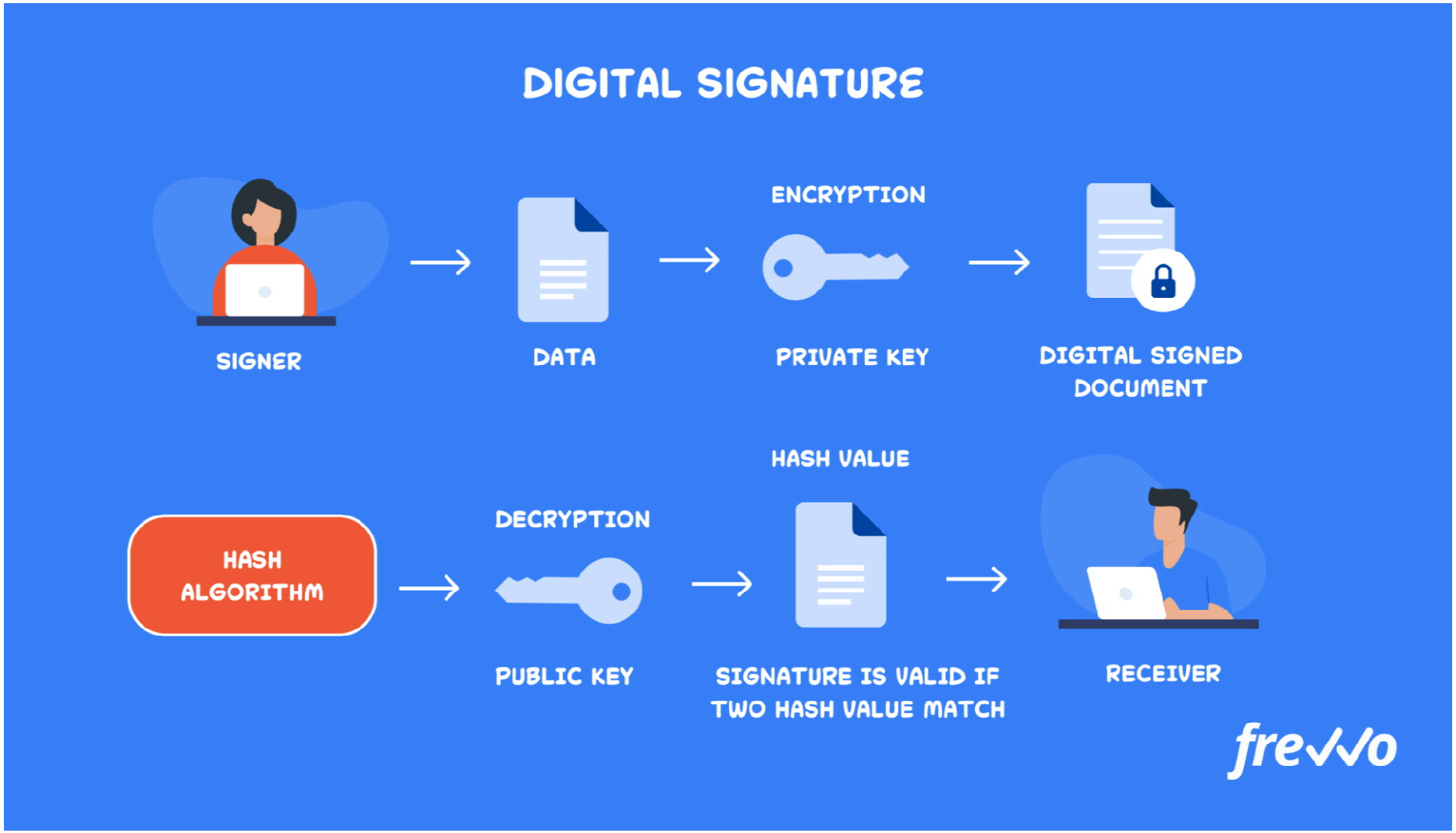
- A digital signature is **a cryptographic output used to verify the authenticity of data**.
- A digital signature algorithm allows for two distinct operations: a signing operation, which uses a signing key to produce a signature over raw data.

Digital Signature

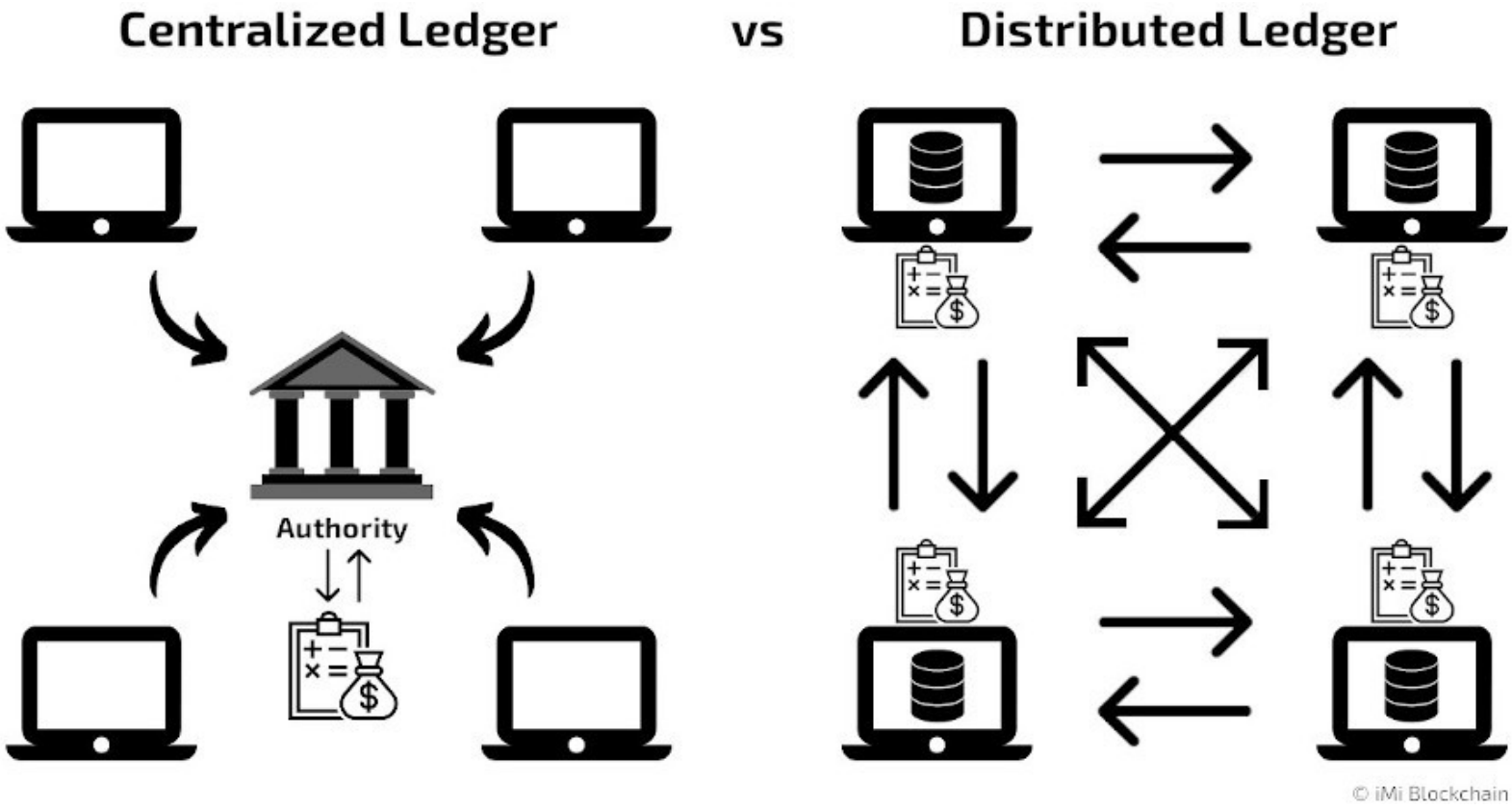


Simplified digitally signed transaction on blockchain.




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



The Properties of Distributed Ledger Technology (DLT)

Programmable
A blockchain is programmable (i.e. Smart Contracts)

Distributed
All network participants have a copy of the ledger for complete transparency

Secure
All records are individually encrypted

Immutable
Any validated records are irreversible and cannot be changed

Anonymous
The identity of participants is either anonymous or pseudonymous

Unanimous
All network participants agree to the validity of each of the records

Time-stamped
A transaction timestamp is recorded on a block

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.

॥ त्वं ज्ञानमयो विज्ञानमयोऽसि ॥

Thank you!