Universidad Politécnica de Cartagena

MIEMBRO DE EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

MINISTERIO DE CIENCIA E INNOVACIÓN

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

AGENCIA ESTATAL DE INVESTIGACIÓN

smartDUMP

BLOCKCHAIN FOR IoT AND DATA SECURITY

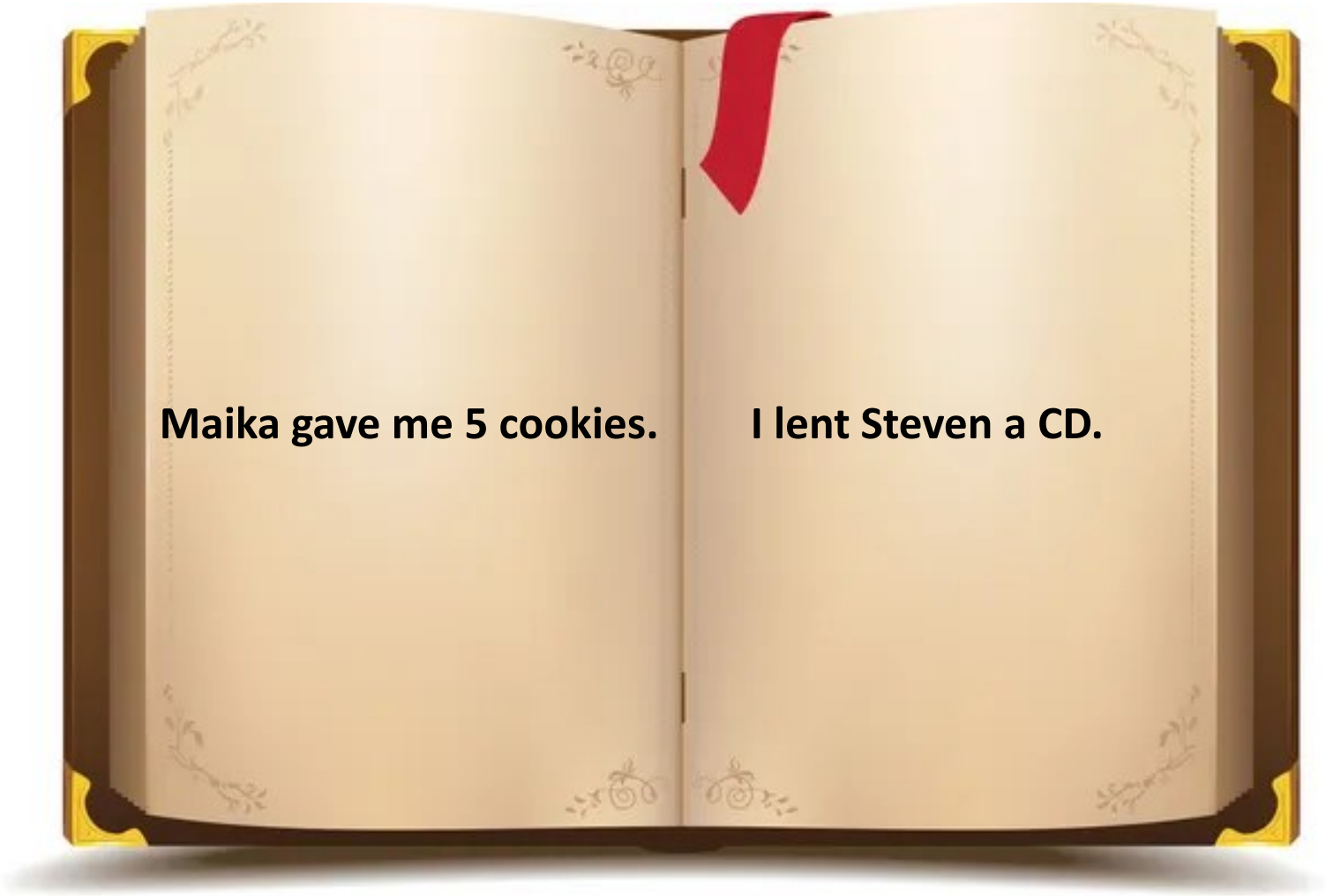
LAURA GARCÍA GARCÍA

Índice

Part 1.

What is Blockchain?

Blockchain



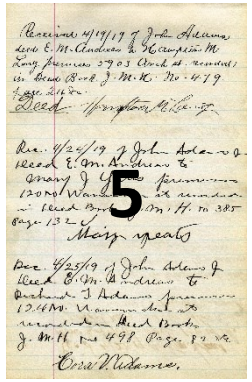
Blockchain

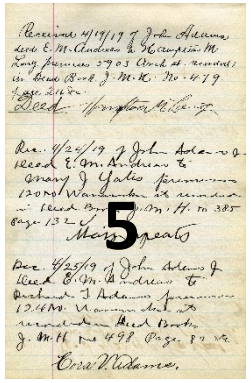
Received 4/19/19 of John Adams deed E. M. Andreas to Hampton M. Long premises 5903 Arch st. recorded in Deed Book J. M. H. No. 479. page 216 &c.
Deed Hampton M. Long

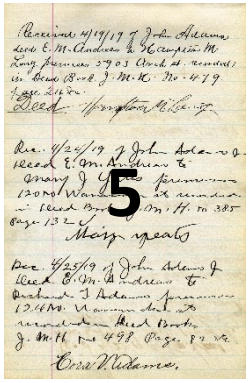
Rec. 4/24/19 of John Adams Jr deed E. M. Andreas to Mary J Yates premises 1200 Wanamaker st recorded in Deed Book J. M. H. no 385 Page 132
Mary Yeates

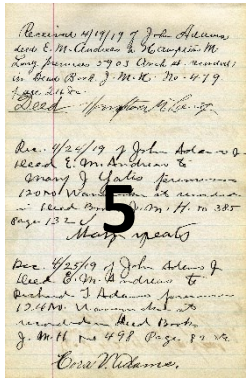
Rec. 4/25/19 of John Adams Jr deed E. M. Andreas to Richard T. Adams premises 1246 N. Wanamaker st recorded in Deed Book J. M. H. no. 498 Page 82 &c
Cora V. Adams.

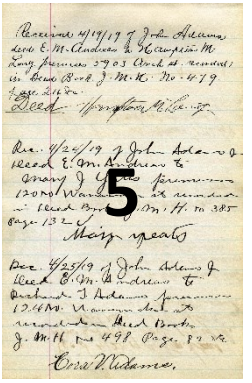
Blockchain











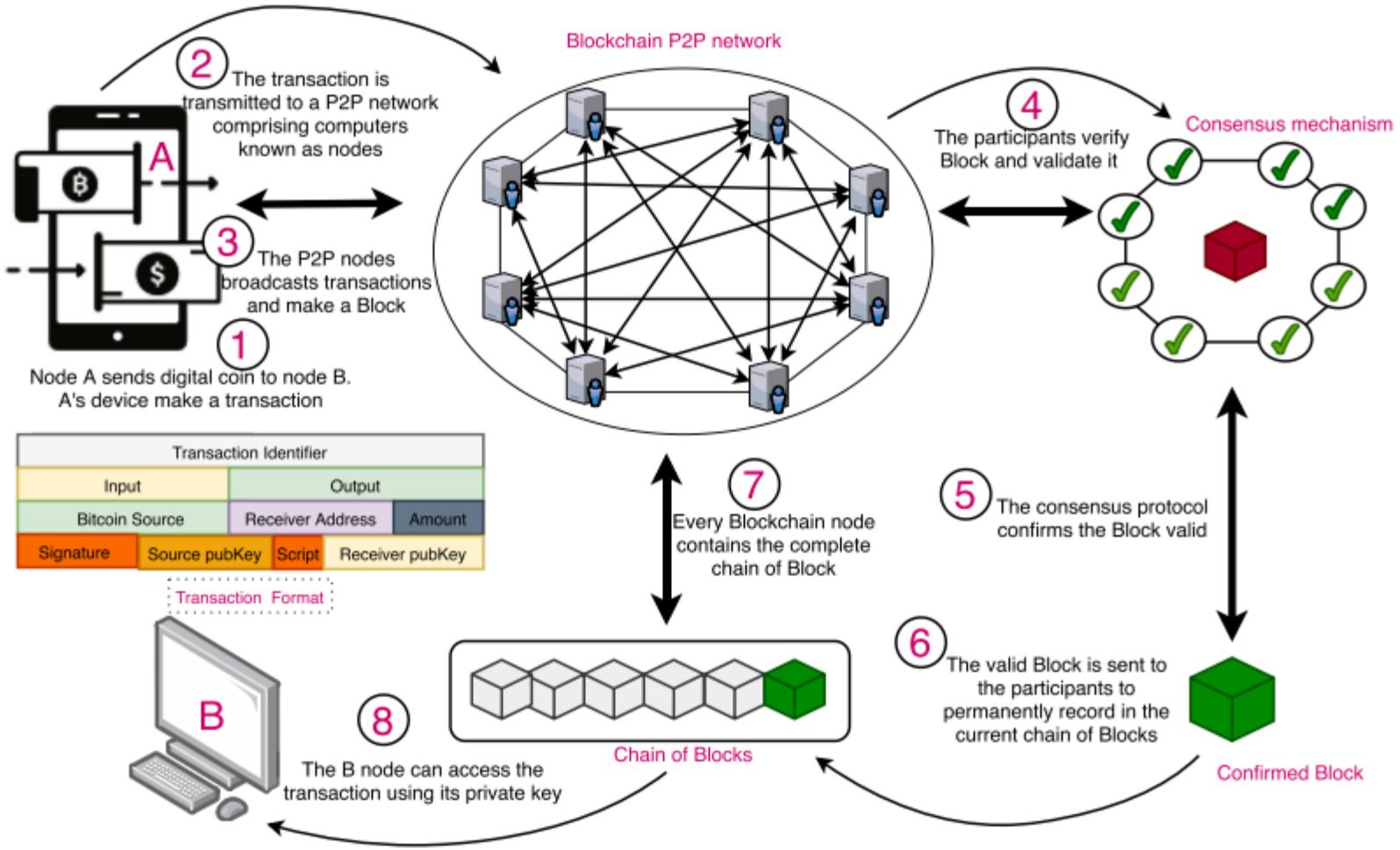
Blockchain

Distributed database

Shared

Immutable

How blockchain works



Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2021). A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain: Research and Applications*, *2*(2), 100006.

First concept: Encryption and Hashing

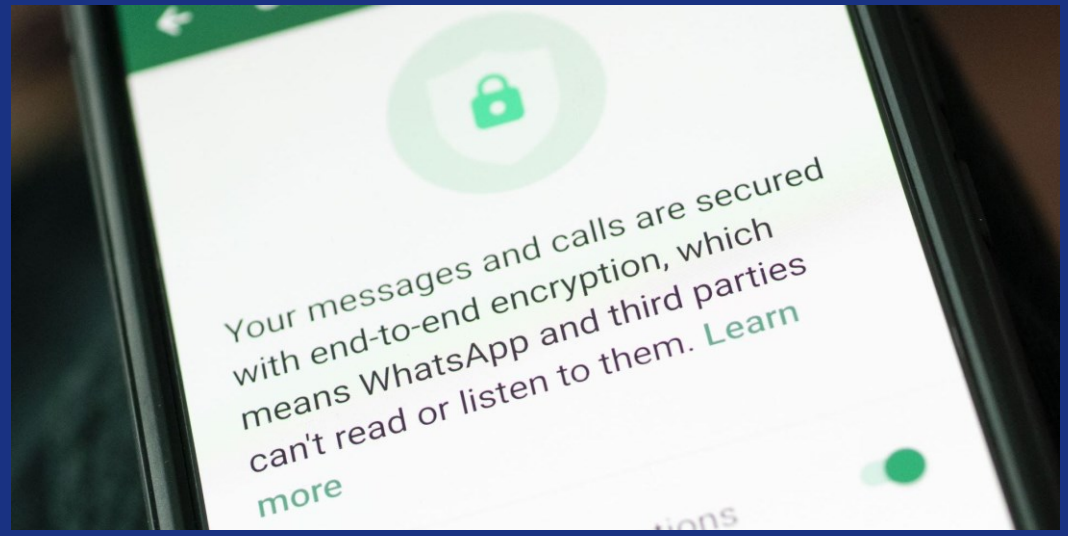
ENCRYPTION

PLAIN TEXT

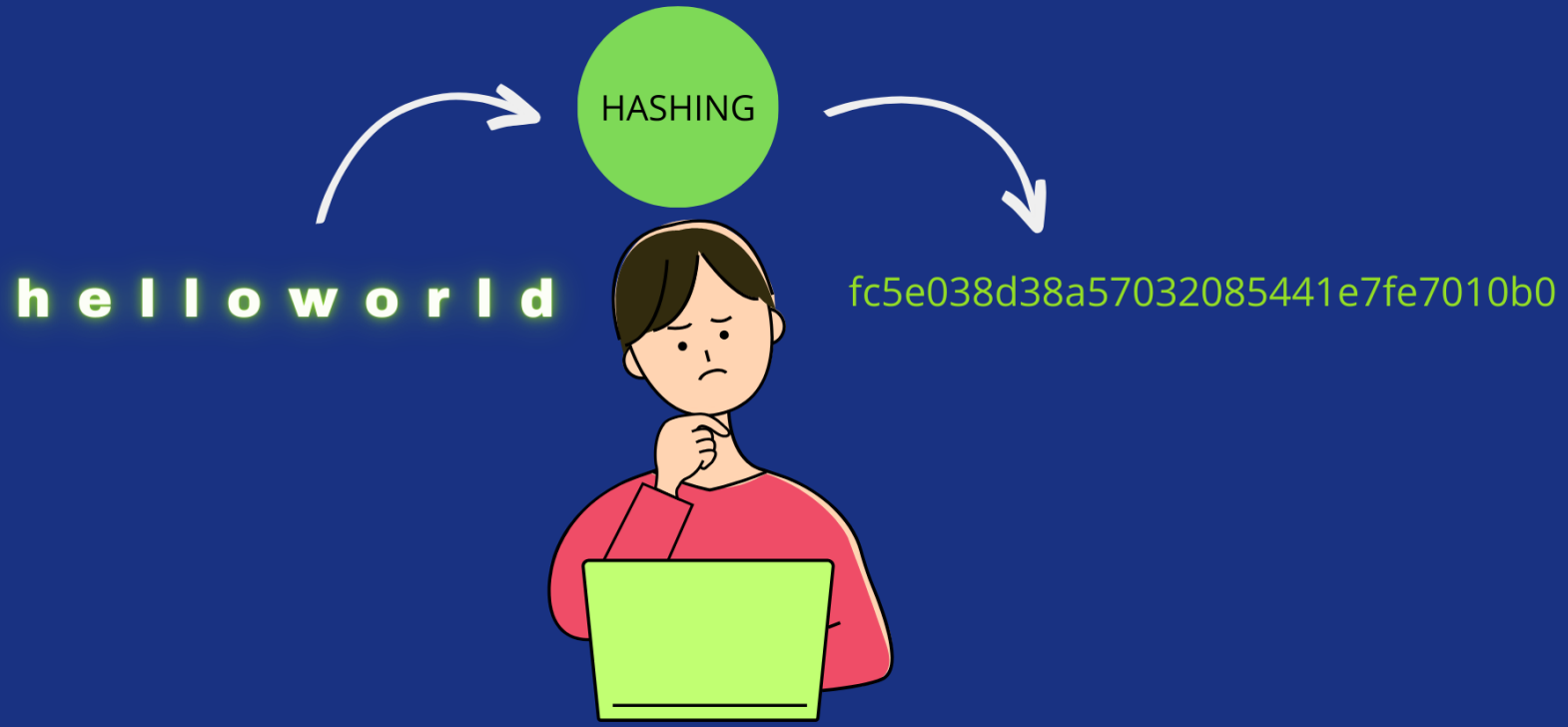
ENCRYPTED TEXT

PLAIN TEXT

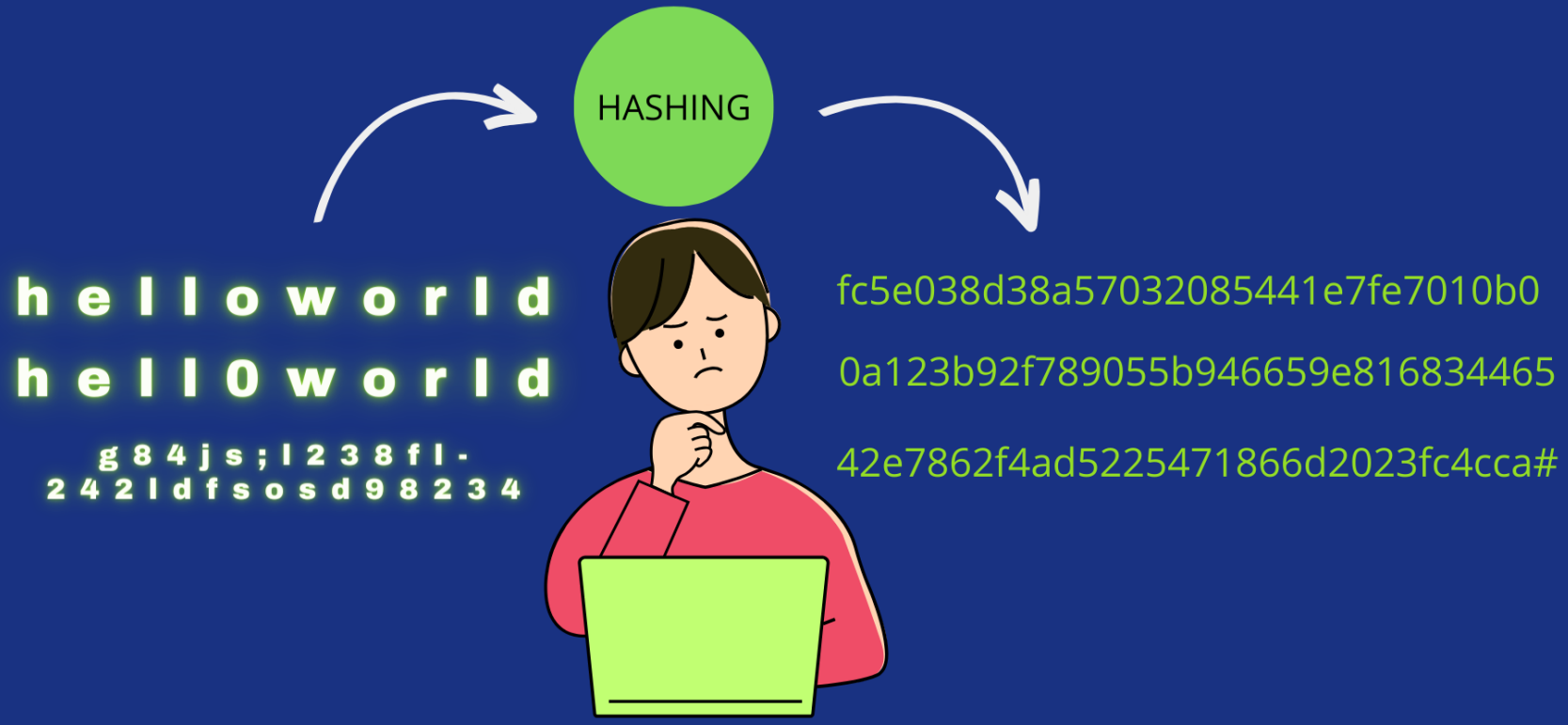
ENCRYPTION


Your messages and calls are secured with end-to-end encryption, which means WhatsApp and third parties can't read or listen to them. Learn more

HASHING



HASHING


HASHING
helloworld
hellOworld
g84js;l238fl-
242ldfsosd98234
fc5e038d38a57032085441e7fe7010b0
0a123b92f789055b946659e816834465
42e7862f4ad5225471866d2023fc4cca#

HASHING

IMPOSSIBLE

INPUT

HASH FUNCTION

OUTPUT

EASY

HASHING

1. *Data Verification:* A hash is a distinct, unchanging string generated from data, often used to verify the integrity of data.

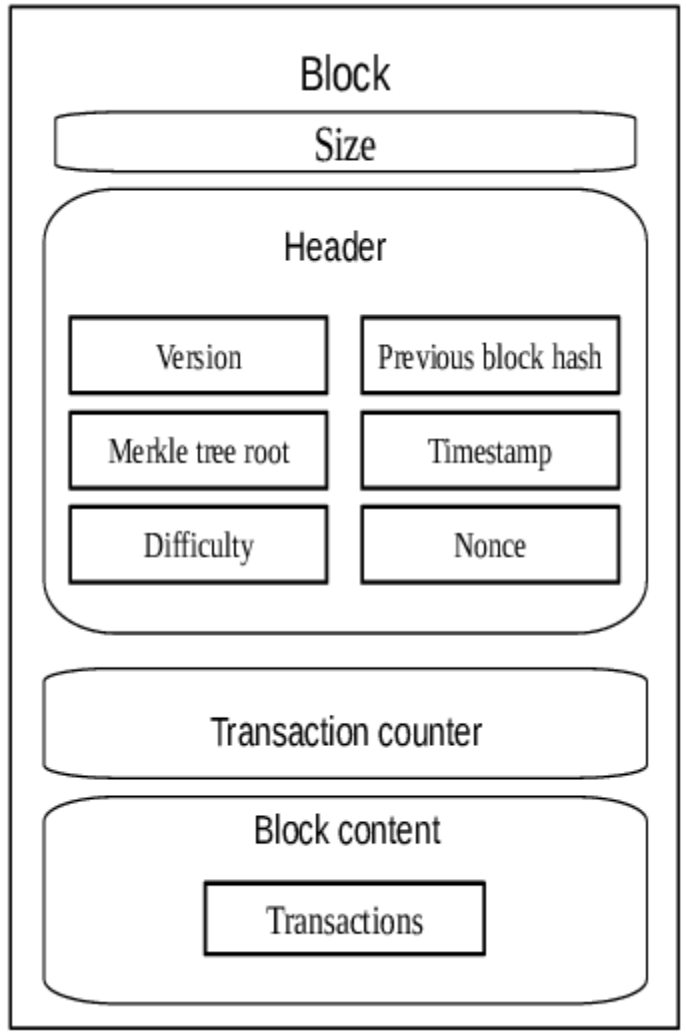
2. *Enhanced Security:* Hashing enhances network security by providing a unique digital fingerprint for data.

3. *Efficient Verification:* Hashes allow for efficient data verification, making alterations detectable.

4. *Data Integrity:* Hashes are used to ensure the integrity of stored data and to maintain the reliability of the network.

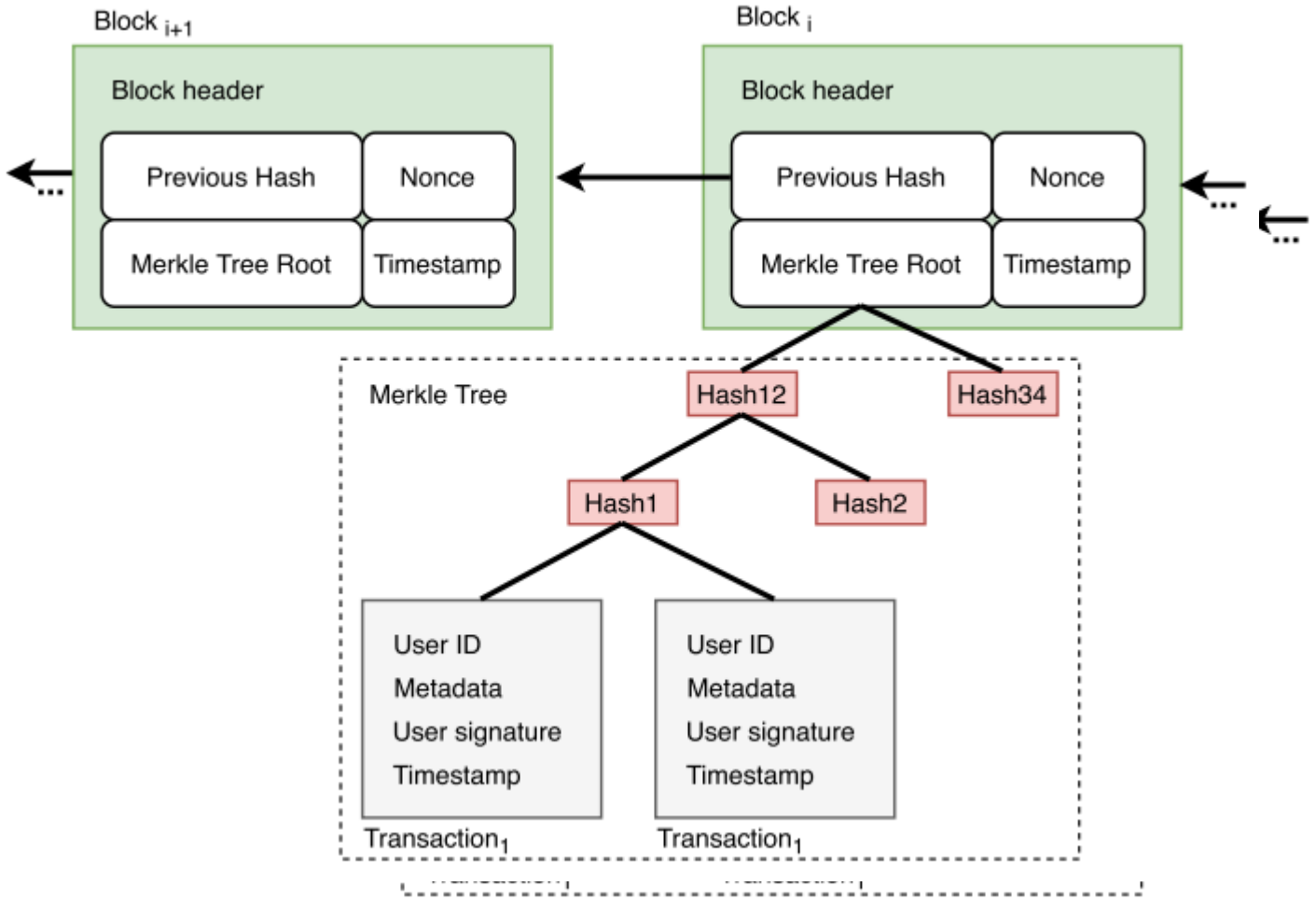
What are blocks?

Structure of a Block



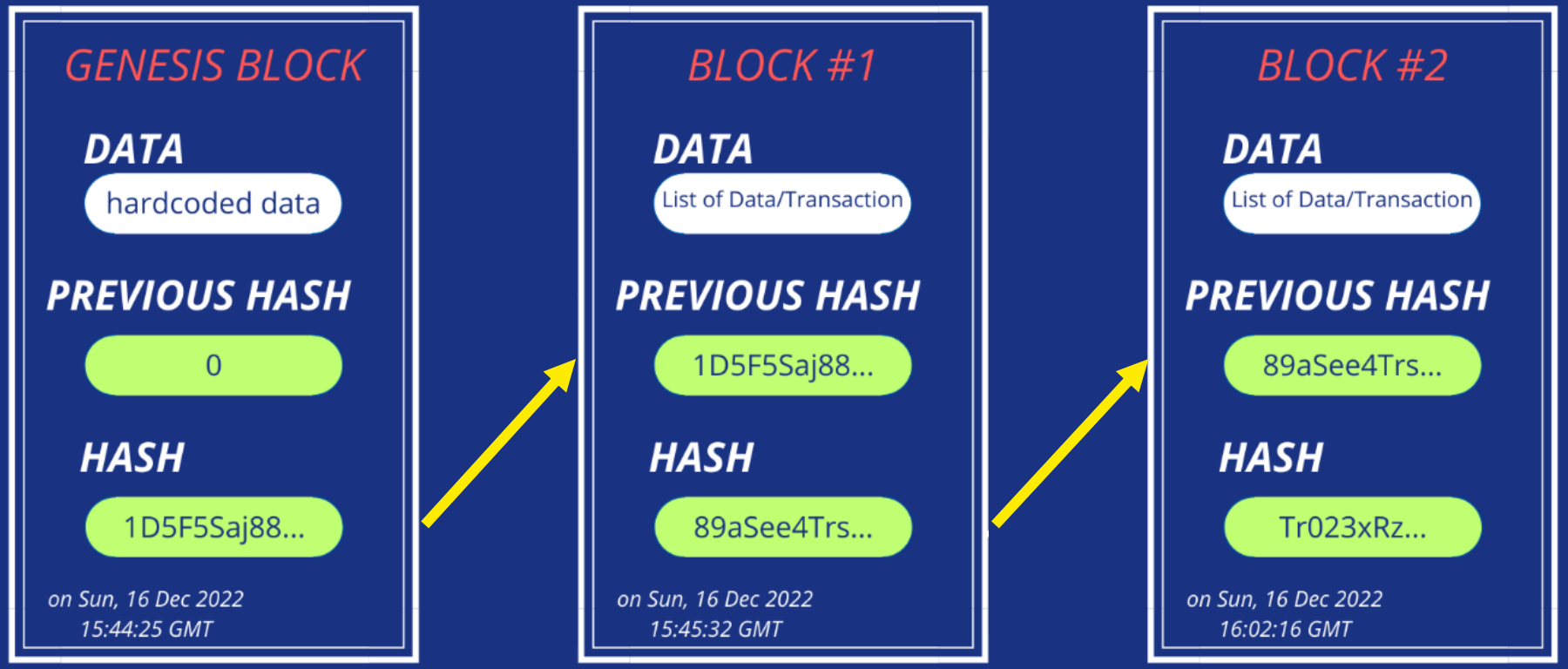
Basegio, T. L., Michelin, R. A., Zorzo, A. F., & Bordini, R. H. (2018). A decentralised approach to task allocation using blockchain. In *Engineering Multi-Agent Systems: 5th International Workshop, EMAS 2017, Sao Paulo, Brazil, May 8-9, 2017, Revised Selected Papers 5* (pp. 75-91). Springer International Publishing.

Structure of a Block



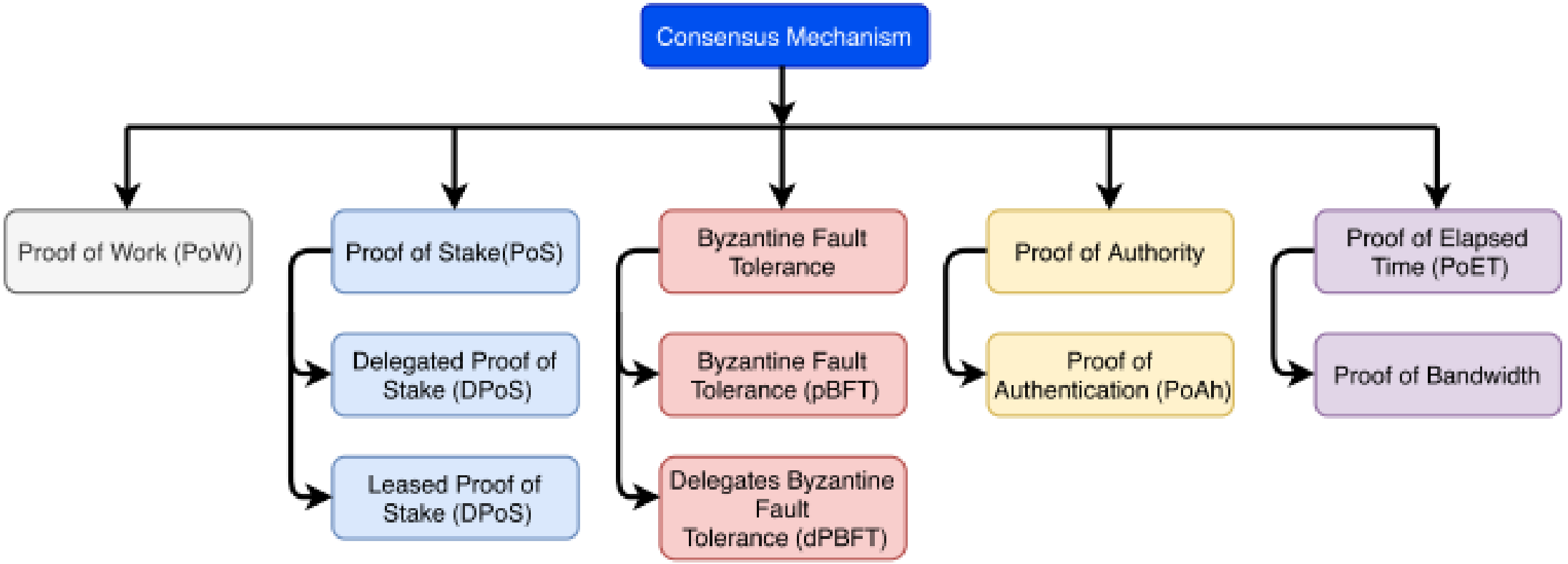
Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2021). A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain: Research and Applications*, *2*(2), 100006.

DATA IN THE BLOCKCHAIN



Consensus protocols

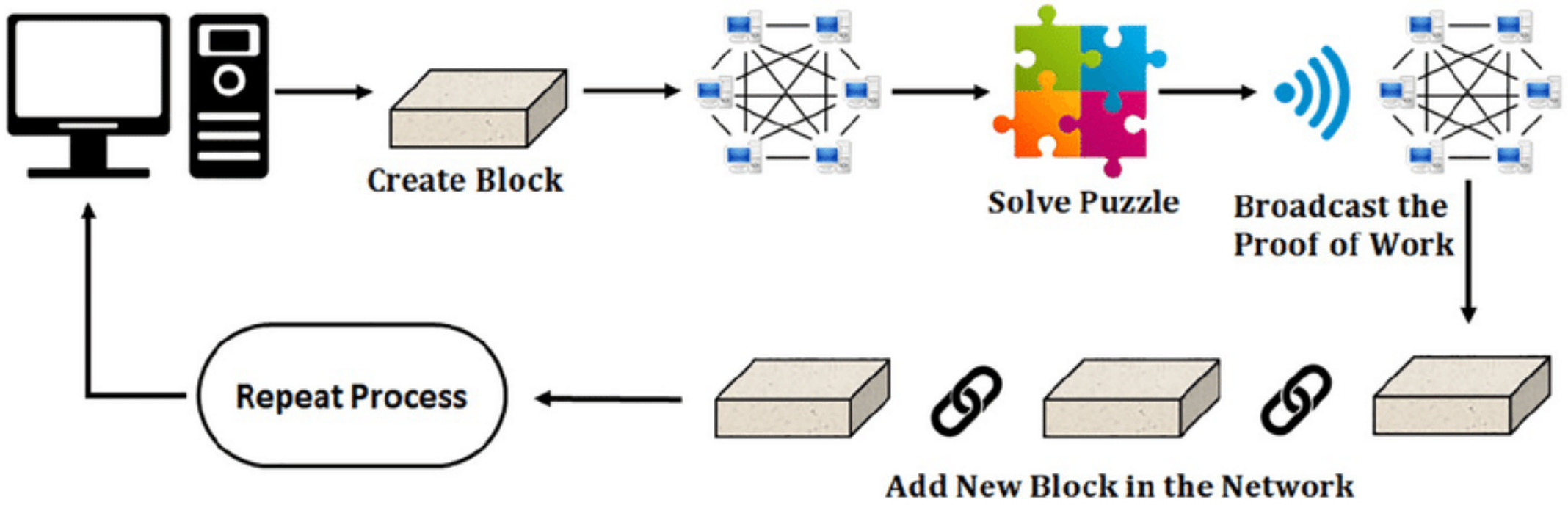
Consensus protocols



Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2021). A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain: Research and Applications*, *2*(2), 100006.

Consensus protocols

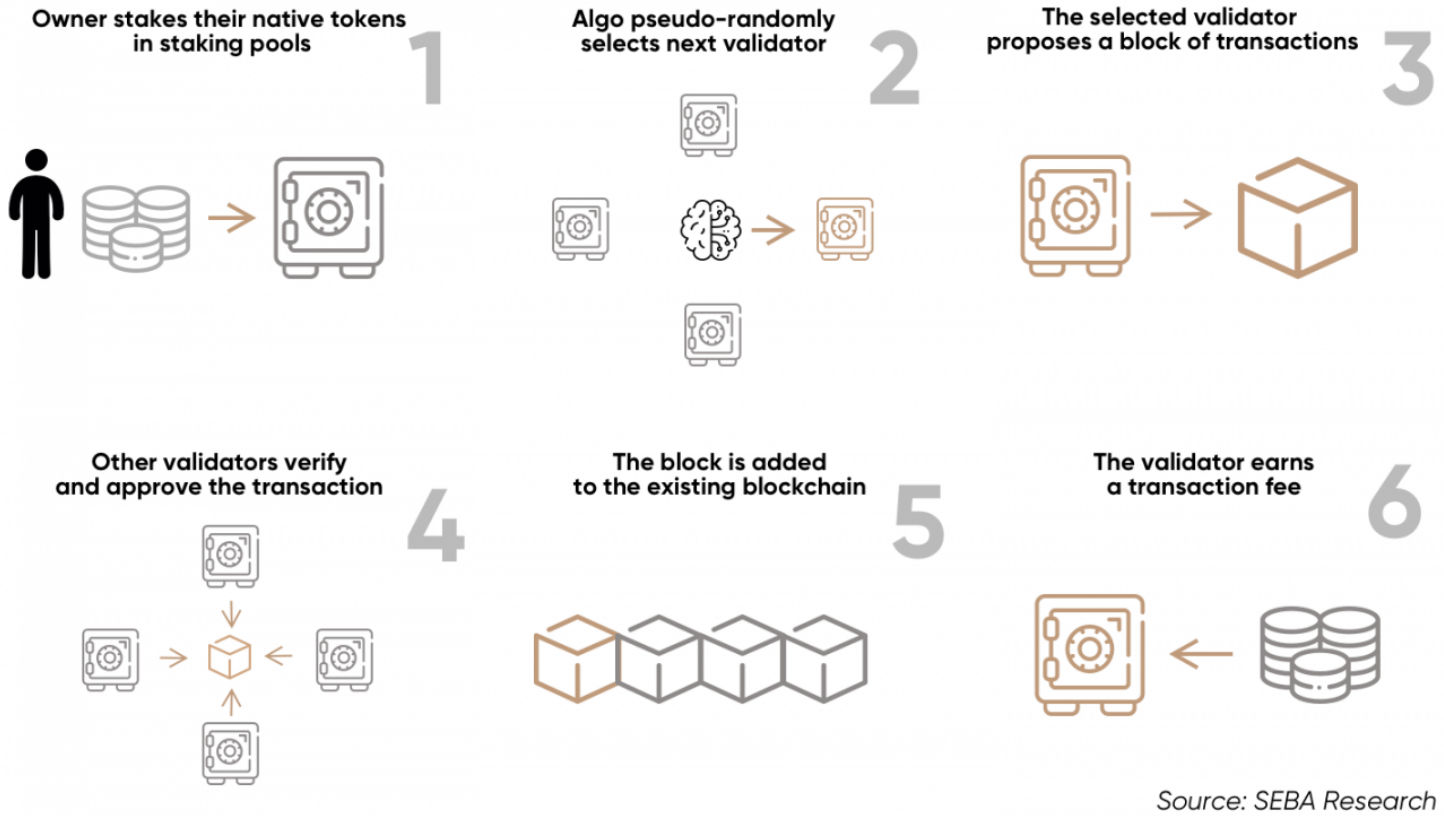
Proof of Work (PoW) → Bitcoin



Latif, S., Idrees, Z., e Huma, Z., & Ahmad, J. (2021). Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions. *Transactions on Emerging Telecommunications Technologies*, *32*(11), e4337.

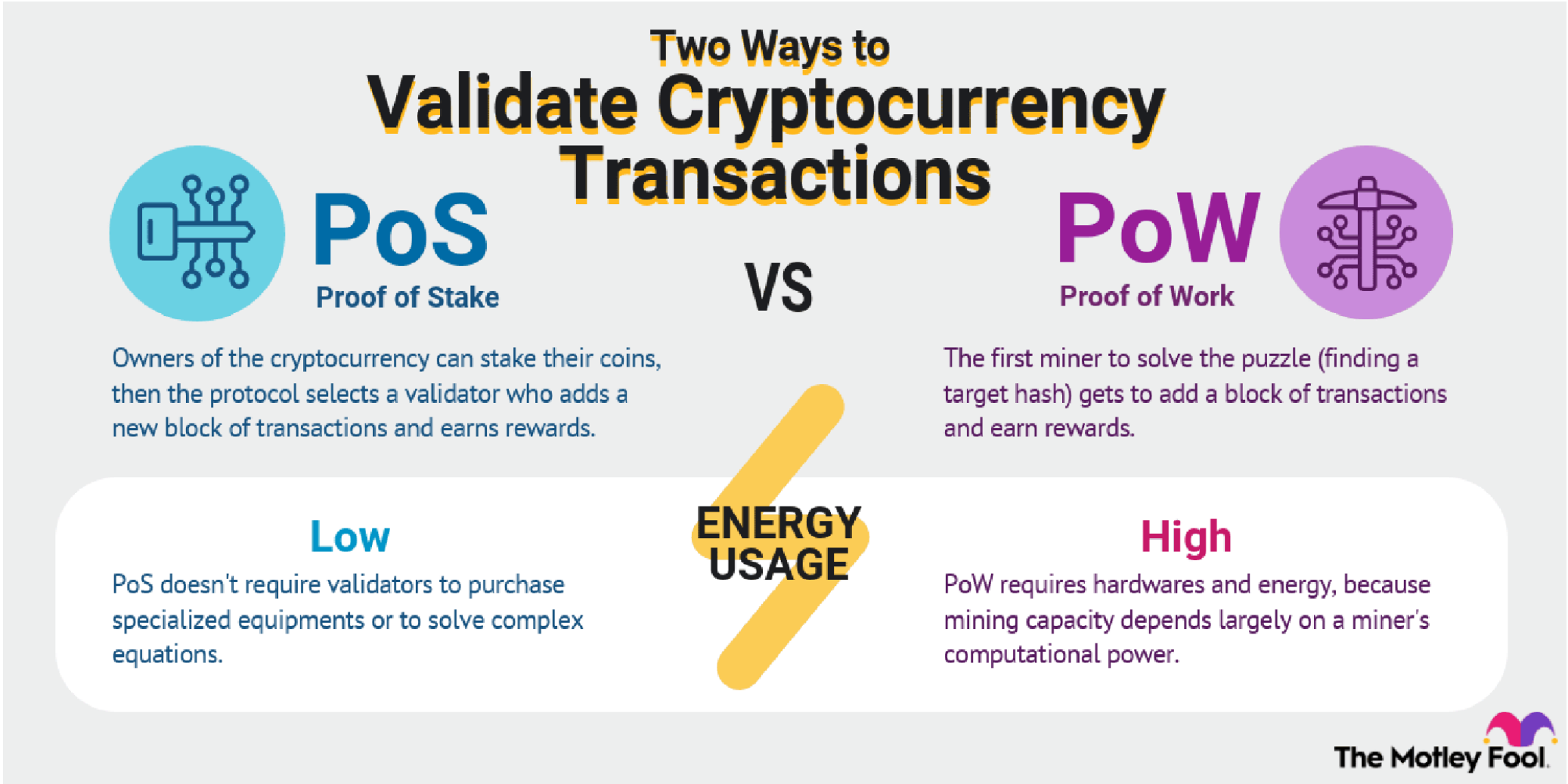
Consensus protocols

Proof of Stake (PoS) → Ethereum



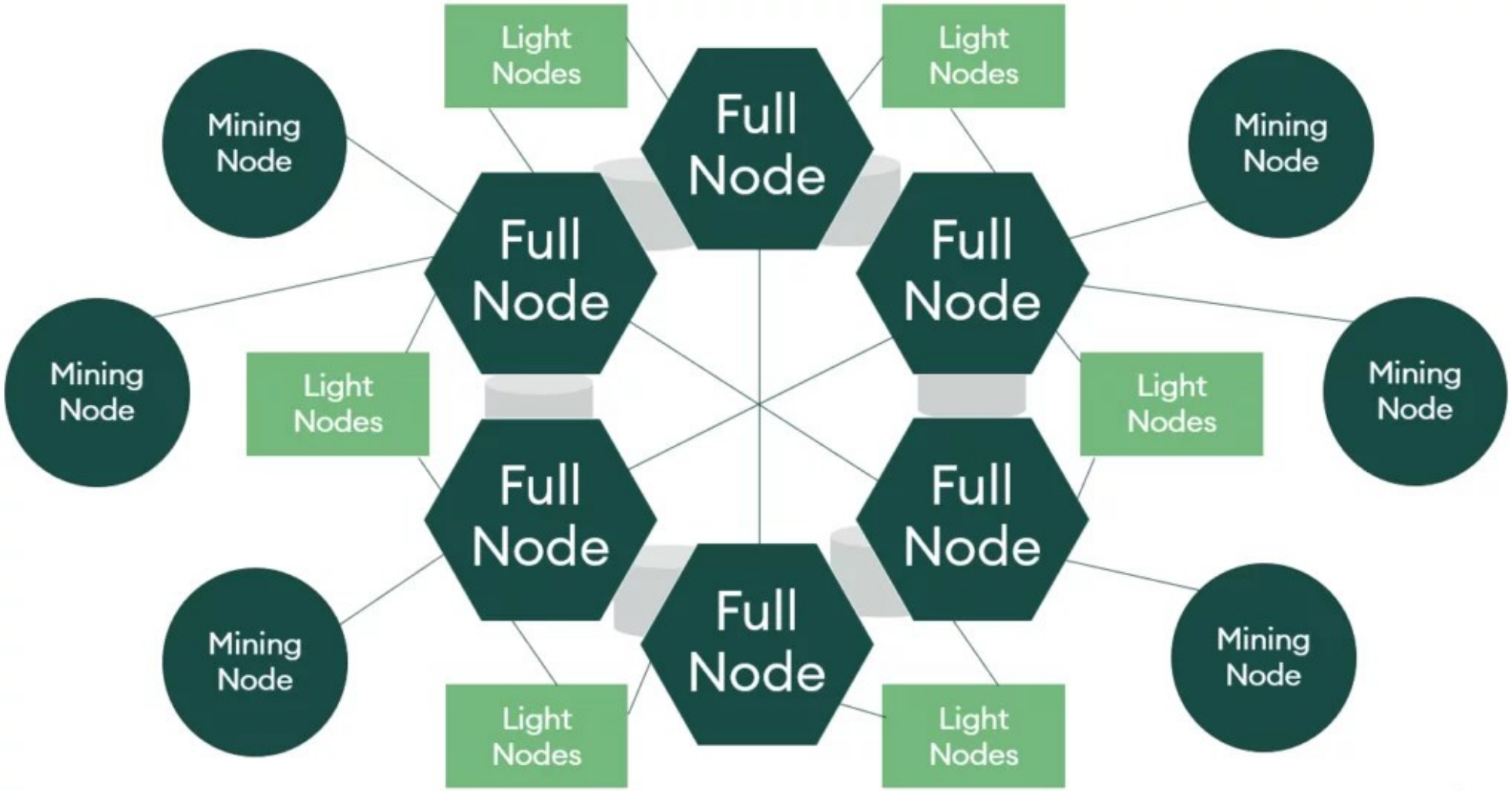
Source: SEBA Research

Consensus protocols

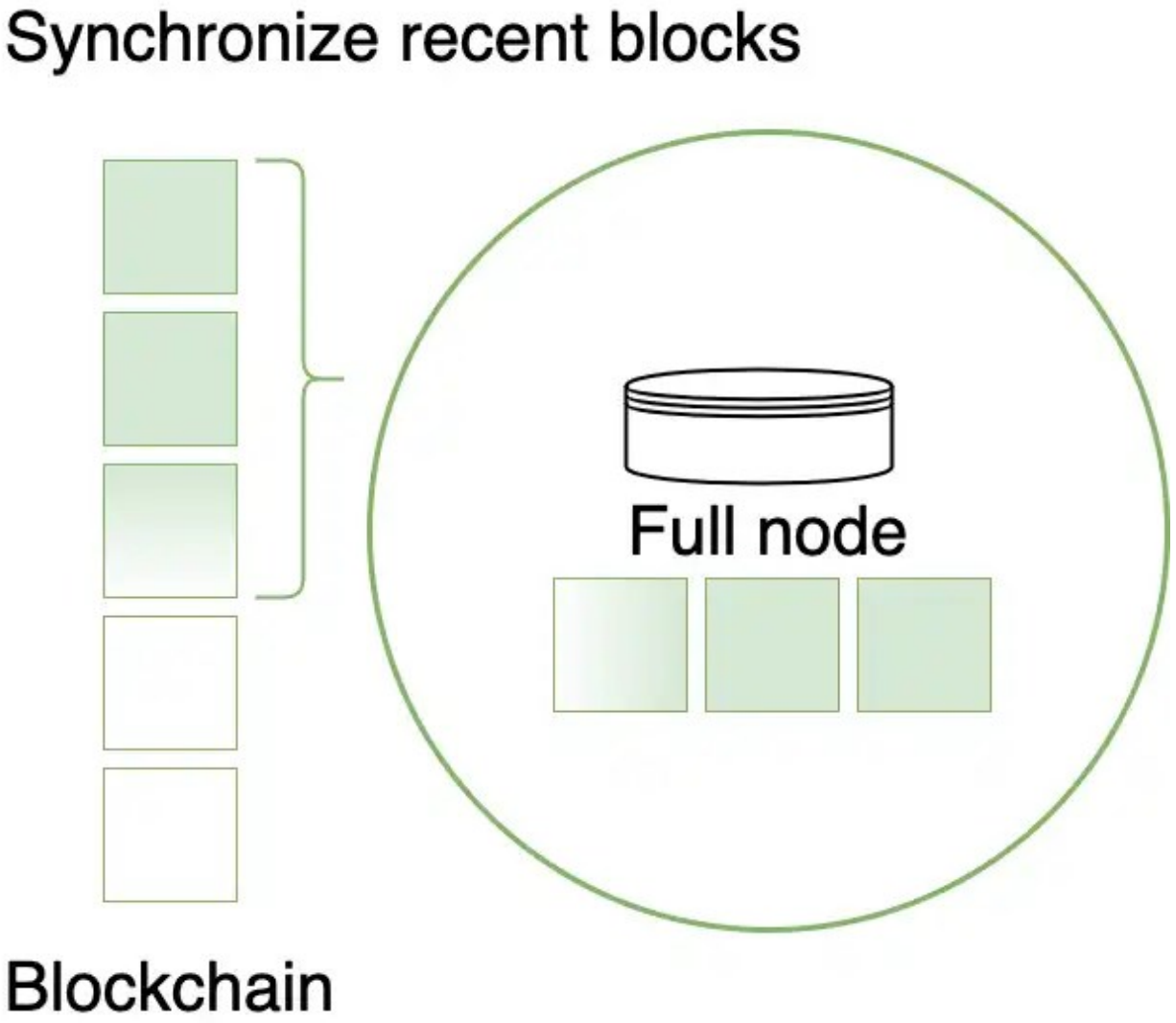


Nodes

Nodes


Light Nodes
Light Nodes
Mining Node
Mining Node
Full Node
Full Node
Full Node
Mining Node
Mining Node
Light Nodes
Light Nodes
Mining Node
Full Node
Full Node
Full Node
Mining Node
Light Nodes
Light Nodes

Full Nodes



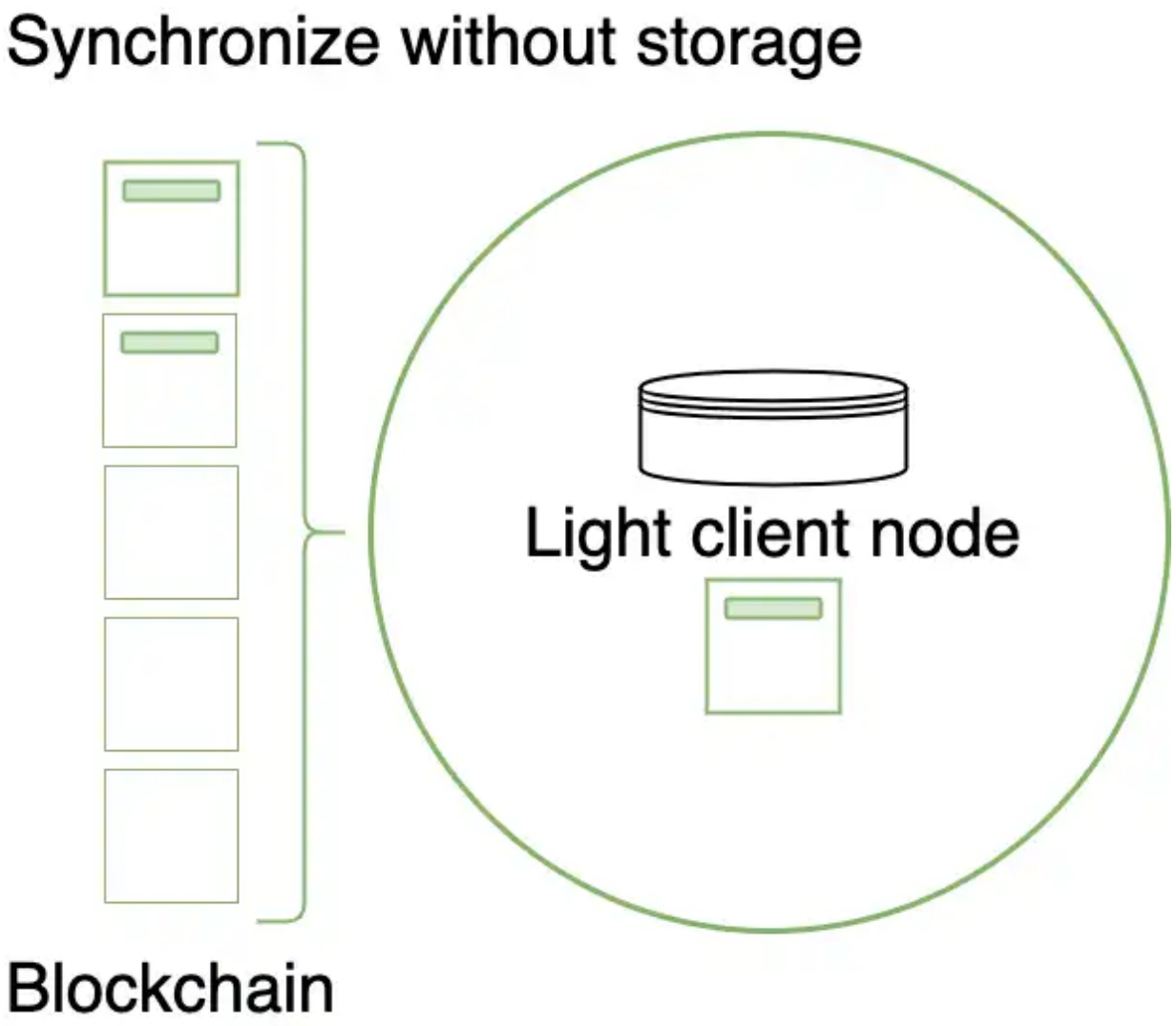
Source: Substrate

Full Nodes

- Store full blockchain data.
- Participate in block validation, verifying all blocks and states.
- All states can be either retrieved from local storage or regenerated from 'snapshots' by a full node.
- Serve the network and provide data on request.

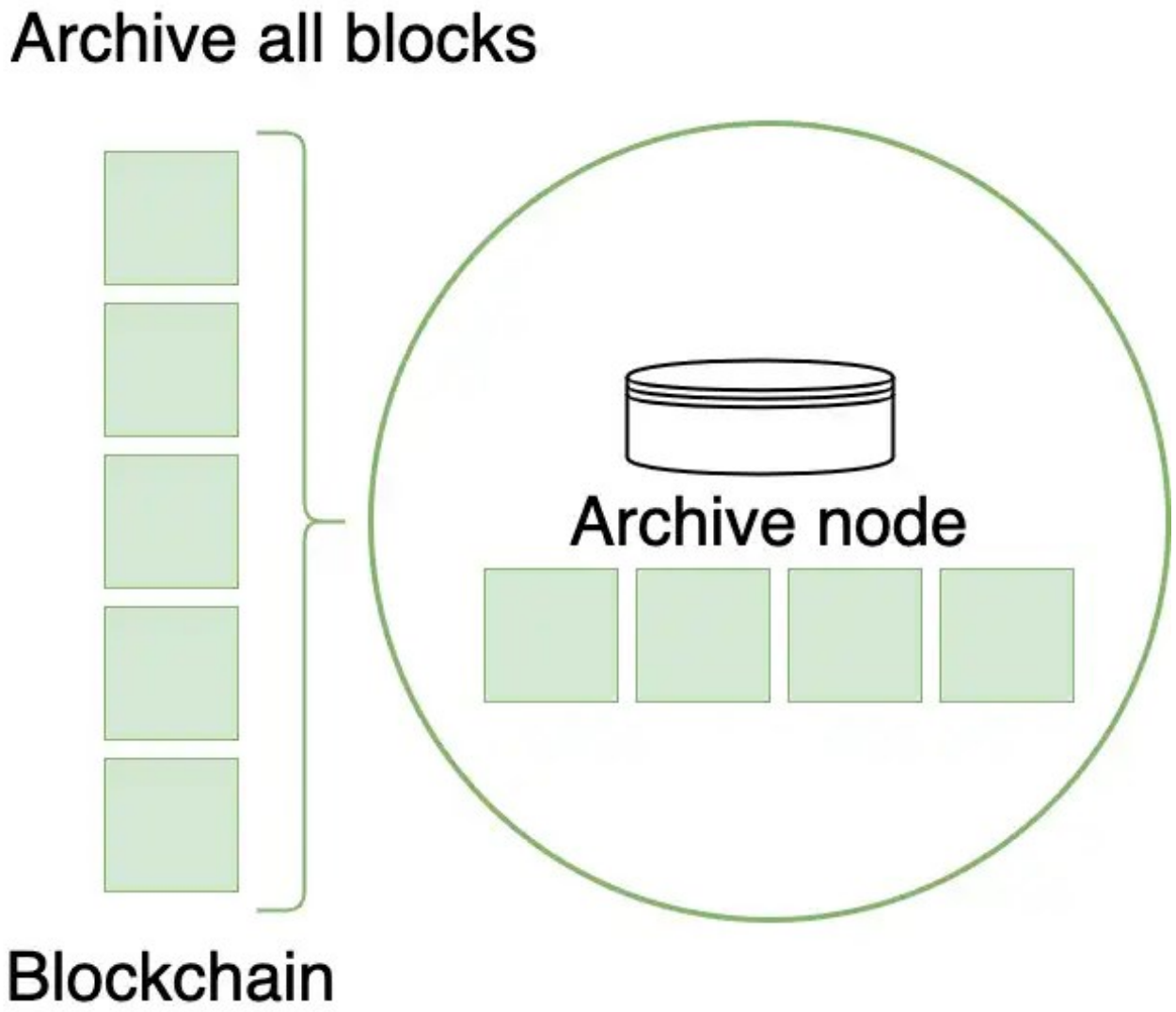
Source: Ethereum documentation

Light Nodes



Source: Substrate

Nodes types



Source: Substrate

Benefits of higher number of nodes in the network

- Full nodes enforce the consensus rules.
- Can perform a social recovery in case of attack.
- Provide robustness.
- Provide access to the blockchain for lightweight nodes.

Clients

A node is made up of two pieces of software (clients) that communicate directly via a JSON-RPC interface and externally via their own P2P interfaces.

Consenus Client

Beacon chain
Beacon state
Execution chain
Operational mempool
P2P Interface

Execution Client

Ethereum Virtual Machine
Execution state
Transaction mempool
P2P Interface

Source: Ethereum

Execution Clients

Client	Language	Operating Systems	Networks	Sync Strategies	State Pruning
Geth	Go	Linux, Windows, macOS	Mainnet, Sepolia, Goerli	Snap, Full	Archive, Pruned
Nethermind	C#, .NET	Linux, Windows, macOS	Mainnet, Sepolia, Goerli, and more	Snap (without serving), Fast, Full	Archive, Pruned
Besu	Java	Linux, Windows, macOS	Mainnet, Sepolia, Goerli, and more	Snap, Fast, Full	Archive, Pruned
Erigon	Go	Linux, Windows, macOS	Mainnet, Sepolia, Goerli, and more	Full	Archive, Pruned
Reth	Rust	Linux, Windows, macOS	Mainnet, Sepolia, Goerli, and more	Full	Archive, Pruned

Consensus Clients

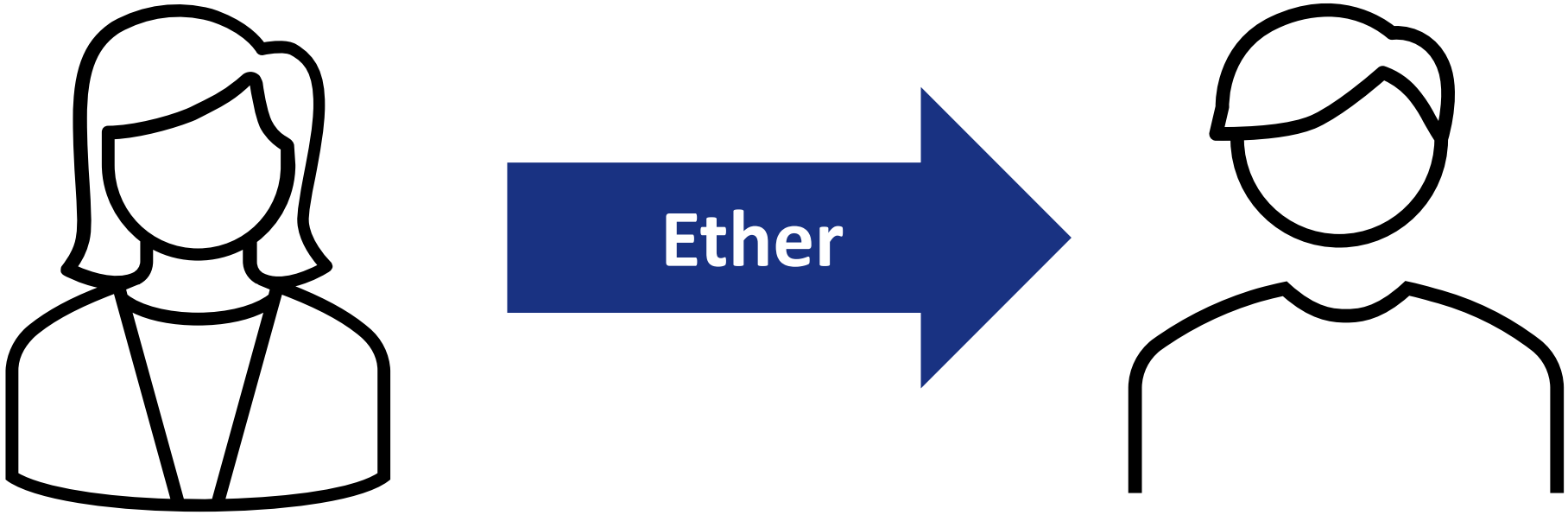
Client	Language	Operating Systems	Networks
Lighthouse	Rust	Linux, Windows, macOS	Beacon Chain, Goerli, Pyrmont, Sepolia, Ropsten, and more
Lodestar	TypeScript	Linux, Windows, macOS	Beacon Chain, Goerli, Sepolia, Ropsten, and more
Nimbus	Nim	Linux, Windows, macOS	Beacon Chain, Goerli, Sepolia, Ropsten, and more
Prysm	Go	Linux, Windows, macOS	Beacon Chain, Gnosis, Goerli, Pyrmont, Sepolia, Ropsten, and more
Teku	Java	Linux, Windows, macOS	Beacon Chain, Gnosis, Goerli, Sepolia, Ropsten, and more

Accounts

Externally-owned	Contract
Creating an account costs nothing.	Creating a contract has a cost because you're using network storage.
Can initiate transactions.	Can only send transactions in response to receiving a transaction.
Transactions between externally-owned accounts can only be ETH/token transfers.	Transactions from an external account to a contract account can trigger code which can execute many different actions, such as transferring tokens or even creating a new contract.
Made up of a cryptographic pair of keys: public and private keys that control account activities.	Contract accounts don't have private keys. Instead, they are controlled by the logic of the smart contract code.

Transactions

What is a transaction?



Maria’s account

Pedro’s account

Information in a Transaction

Information element	Description
From	The address of the sender.
Recipient	The receiving address.
Signature	The identifier of the sender.
Nonce	A counter that is incremented secuencially.
Value	Amount of ETH or coins to transfer from sender to recipient.
InputData	Optional field to include arbitrary data
GasLimit	The maximum amount of gas units that can be consumed by the transaction.
MaxPriorityFeePerGas	The maximum price of the consumed gas to be included as a tip to the validator.
MaxFeePerGas	The maximum fee per unit of gas willing to be paid for the transaction.

Types of Transactions

- **Regular transactions:** a transaction from one account to another.

- **Contract deployment transactions:** a transaction without a 'to' address, where the data field is used for the contract code.

- **Execution of a contract:** a transaction that interacts with a deployed smart contract. In this case, 'to' address is the smart contract address.

Gas and fees (Ethereum) (Transsaction cost)

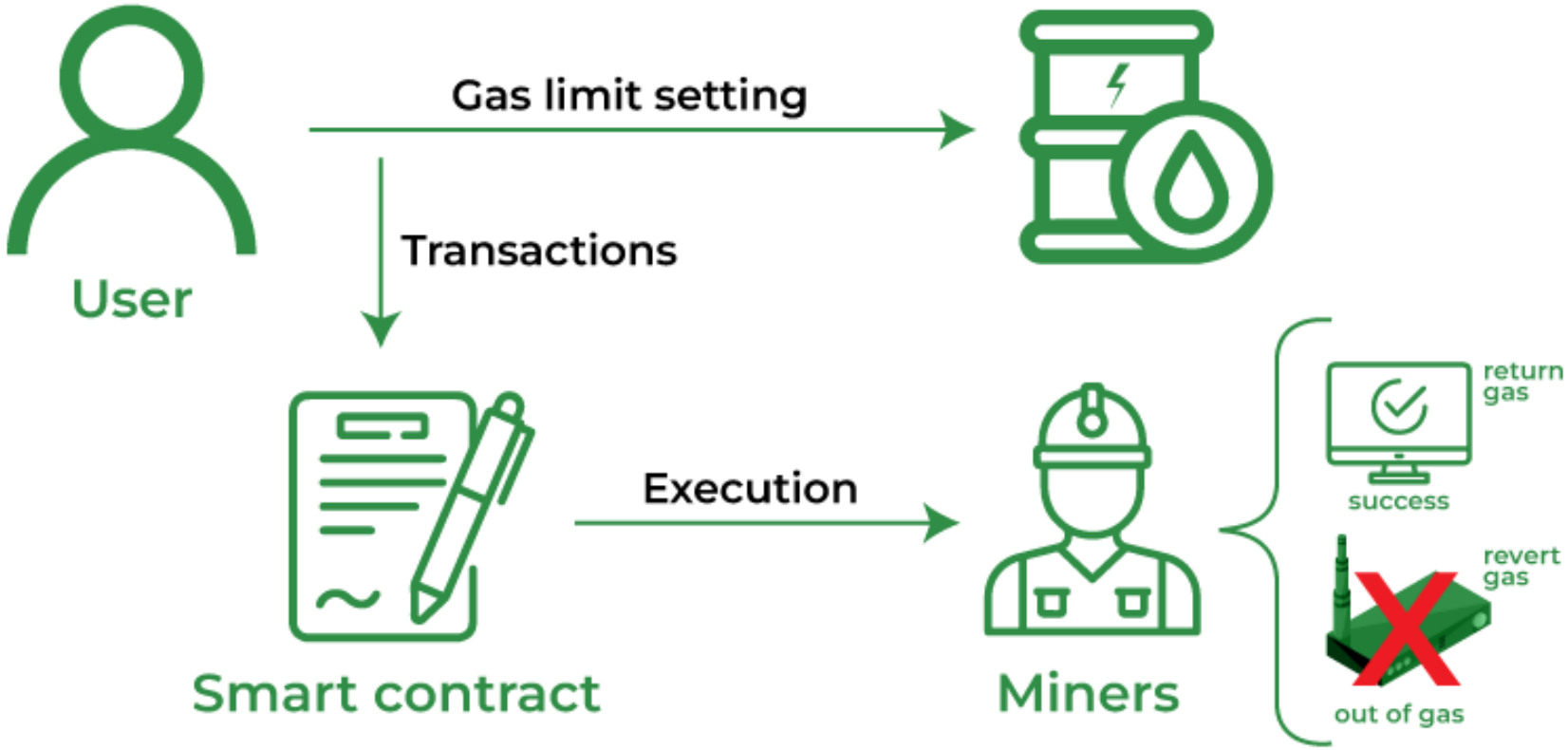
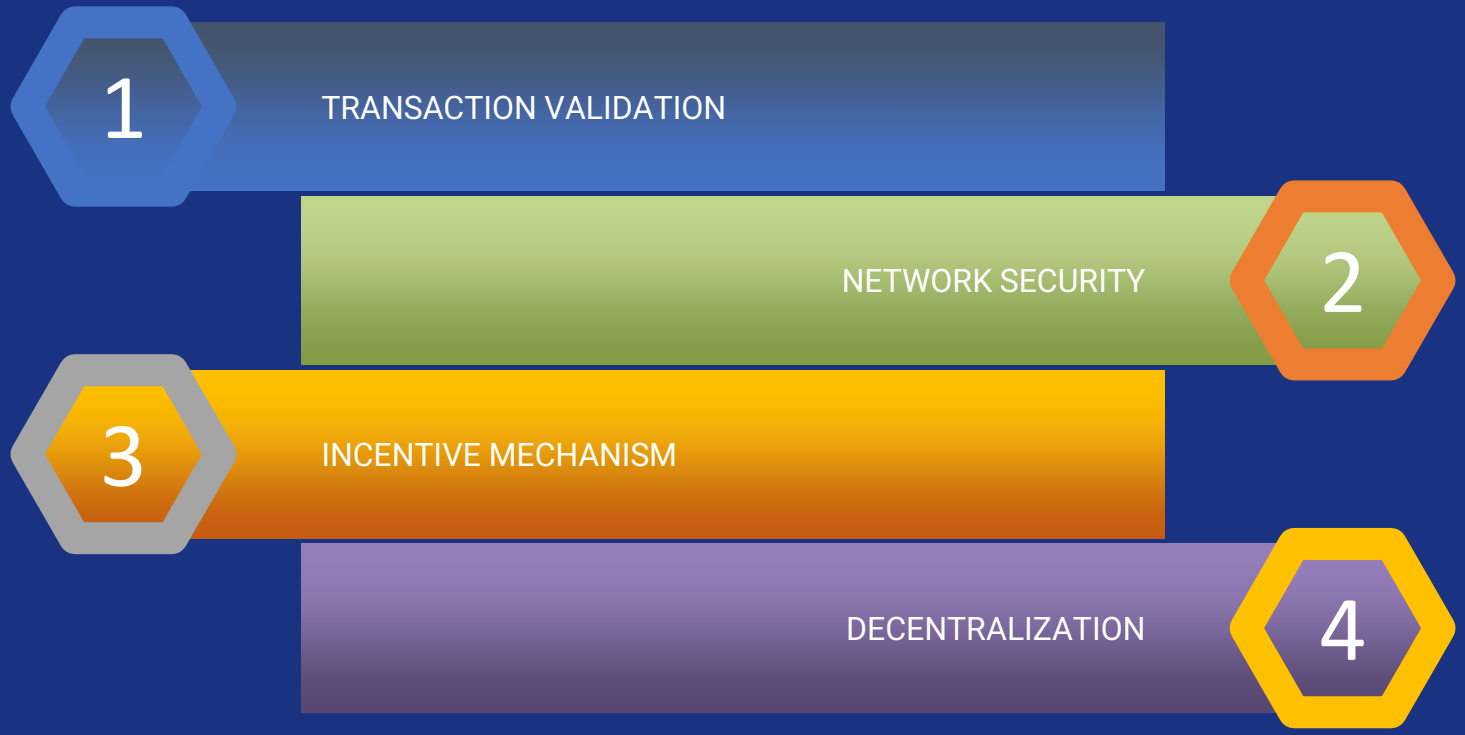


Image source: geeksforgeeks

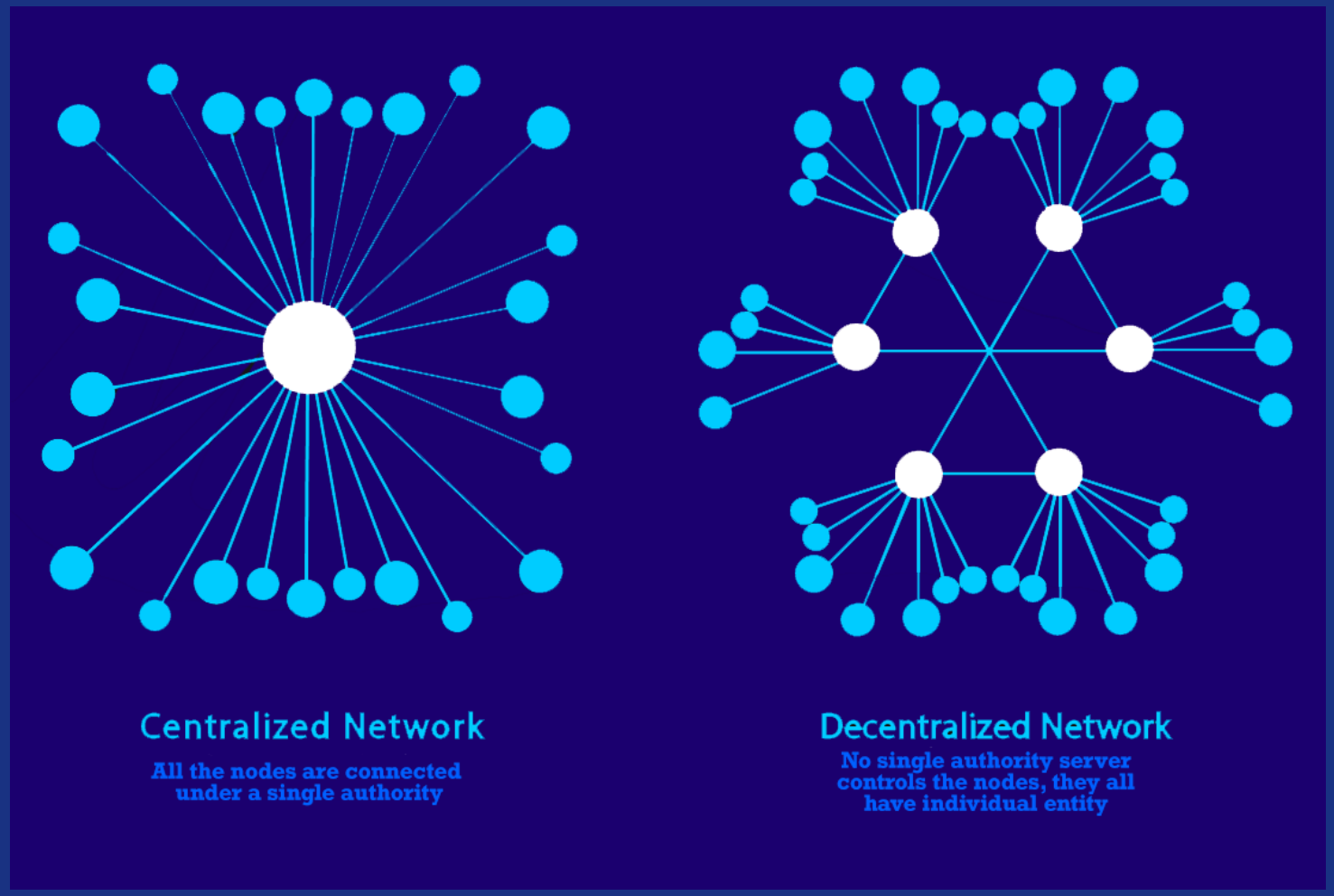
Mining

MINING


1
TRANSACTION VALIDATION
NETWORK SECURITY
2
3
INCENTIVE MECHANISM
DECENTRALIZATION
4

Types of blockchain networks

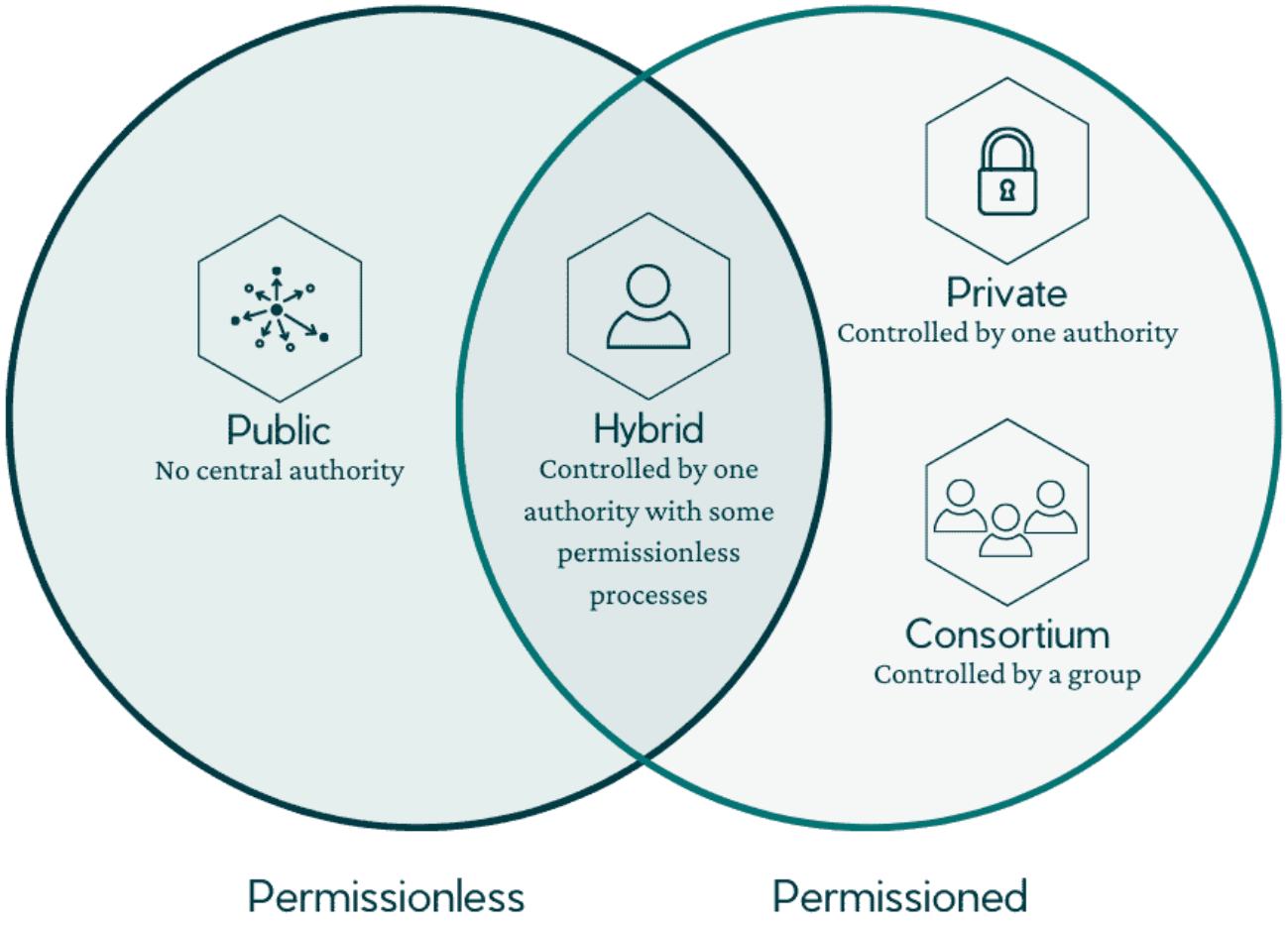
CENTRALIZED VS DECENTRALIZED BLOCKCHAIN



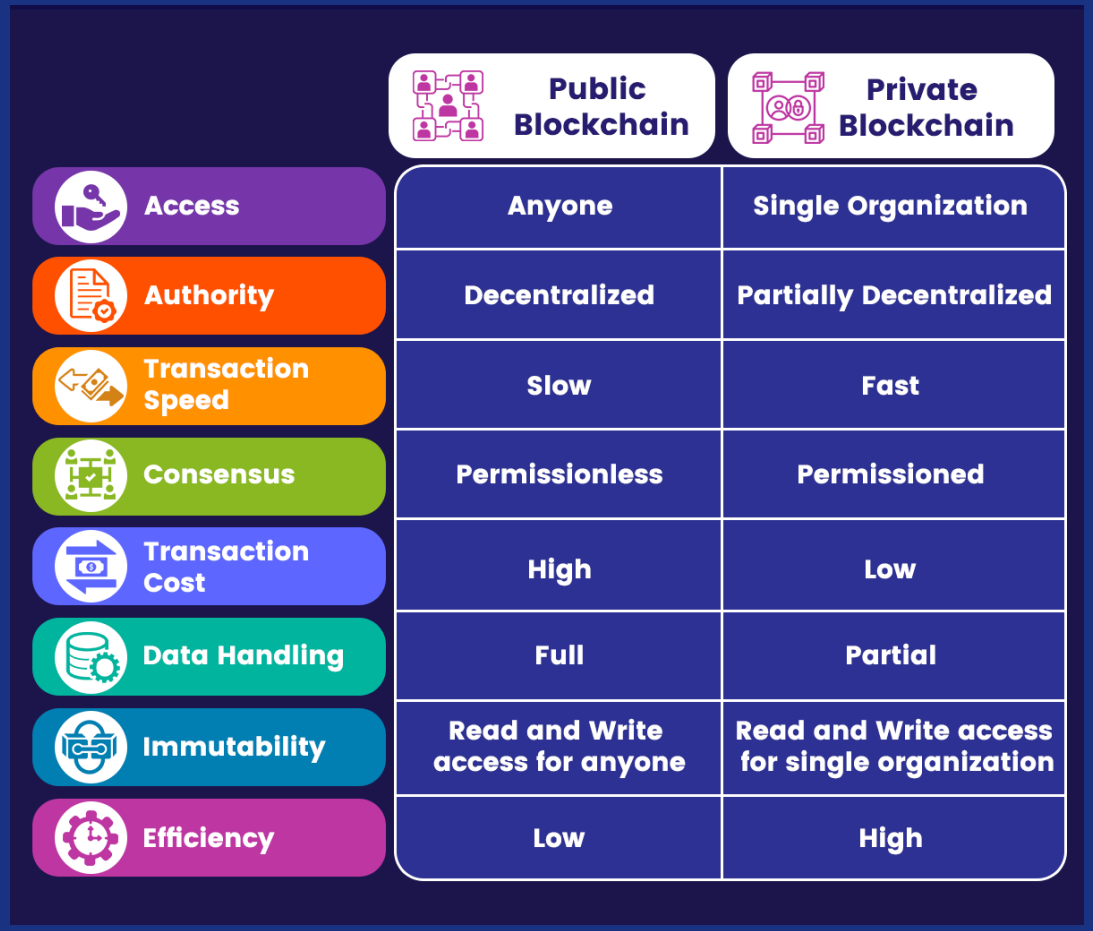
CENTRALIZED VS DECENTRALIZED BLOCKCHAIN

	CENTRALIZED		DESCENTRALIZED
1	• SINGLE VALIDATOR	▷	• MULTIPLE VALIDATORS
2	• CENTRAL AUTHORITY	▷	• DISTRIBUTED AUTHORITY
3	• LIMITED TRANSPARENCY	▷	• FULL TRANSPARENCY
4	• RESTRICTED PARTICIPATION	▷	• FULL PARTICIPATION

Types of blockchain networks



PRIVATE VS PUBLIC BLOCKCHAIN



	Public Blockchain	Private Blockchain
Access	Anyone	Single Organization
Authority	Decentralized	Partially Decentralized
Transaction Speed	Slow	Fast
Consensus	Permissionless	Permissioned
Transaction Cost	High	Low
Data Handling	Full	Partial
Immutability	Read and Write access for anyone	Read and Write access for single organization
Efficiency	Low	High

Ethereum networks

Public Networks

Network	Description
Mainnet	Mainnet is the primary public Ethereum production blockchain, where actual-value transactions occur on the distributed ledger. The Ethers or coins used in this network have real value.
Testnets	These are networks used by protocol developers or smart contract developers to test both protocol upgrades as well as potential smart contracts in a production-like environment before deployment to Mainnet. There are different testnets that use different consensus mechanisms. The coin used in most of these testnets don't have real value.

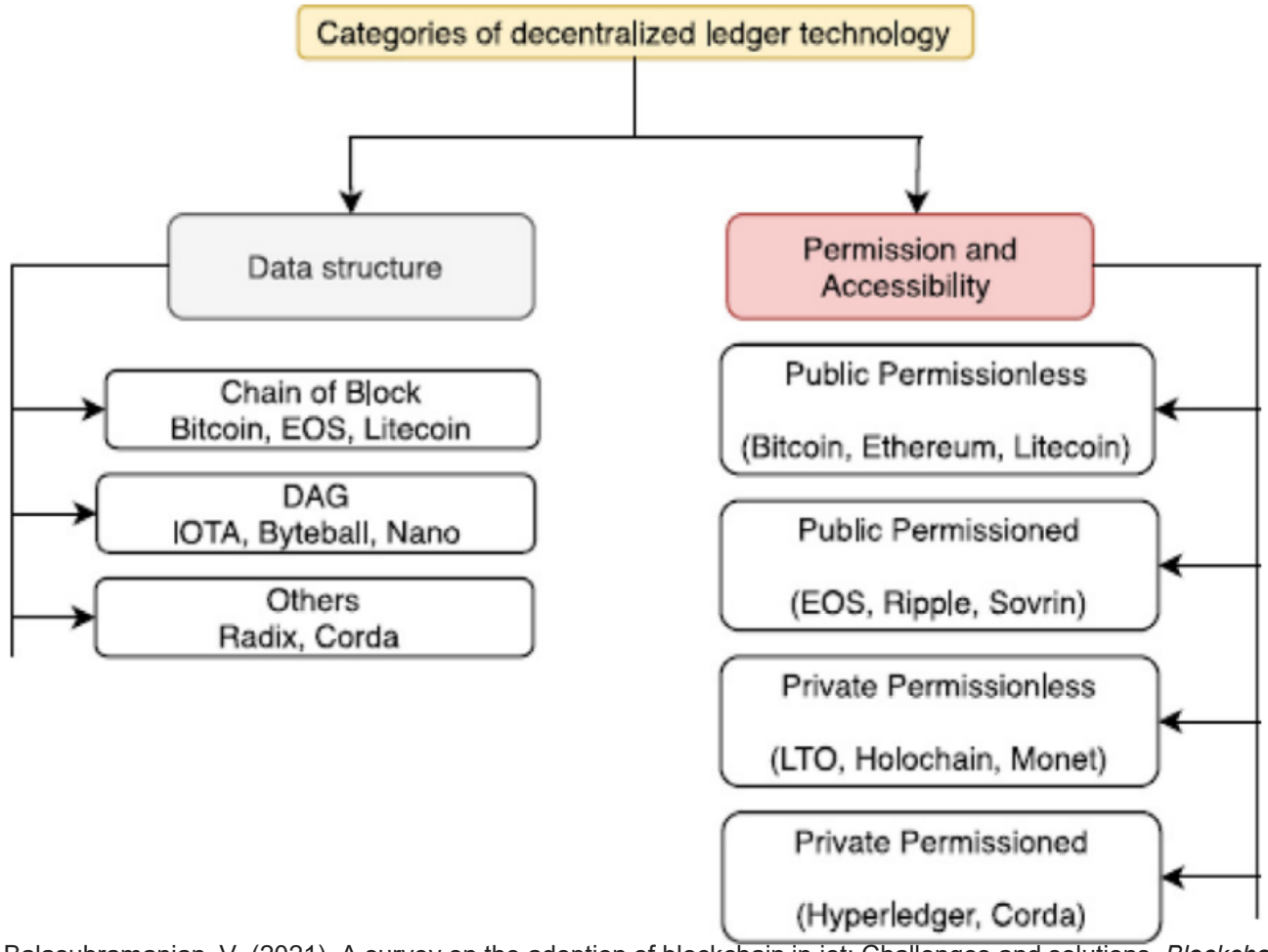
Types of blockchain networks

Private Networks

Network	Description
Development	It is possible to create a local blockchain instance to test decentralized apps and smart contracts.
Consortium	The consensus process is controlled by a pre-defined set of nodes that are trusted.

Key elements of a blockchain

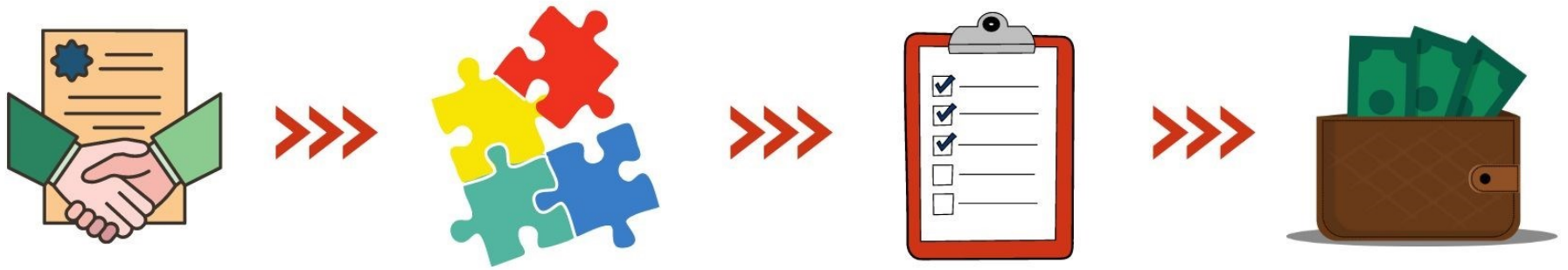
Distributed Ledger Technology



Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2021). A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain: Research and Applications*, *2*(2), 100006.

Smart Contract

How does the Smart Contract work?



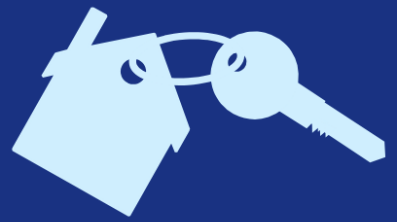
Pre-defined Contract → Business Logic → Execution → Settlement

SMART CONTRACT

RECORD STORING

TRADING ACTIVITIES

SUPPLY CHAIN



MORTGAGE

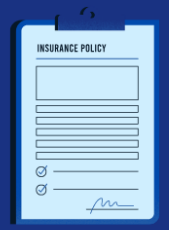
REAL STATE

EMPLOYMENT ARRANGEMENTS

COPYRIGHT PROTECTION

HEALTHCARE

VOTING



INSURANCE CLAIMS

INTERNET OF THINGS

SMART CONTRACT FOR AIR QUALITY IoT

- This could be related to air quality sensors at various city locations, setting a maximum allowable pollution limit.
- If pollution levels exceed that limit, the smart contract could automatically trigger traffic closures in specific areas or throughout the entire city, using verifiable data obtained through blockchain technology.

Smart Contract

SOLIDITY

•Object-oriented, high-level language for implementing smart contracts.
•Curly-bracket language that has been most profoundly influenced by C++.
•Statically typed (the type of a variable is known at compile time).

•Supports:

- Inheritance (you can extend other contracts).
- Libraries (you can create reusable code that you can call from different contracts – like static functions in a static class in other object-oriented programming languages).
- Complex user-defined types.

Smart Contract

VYPER

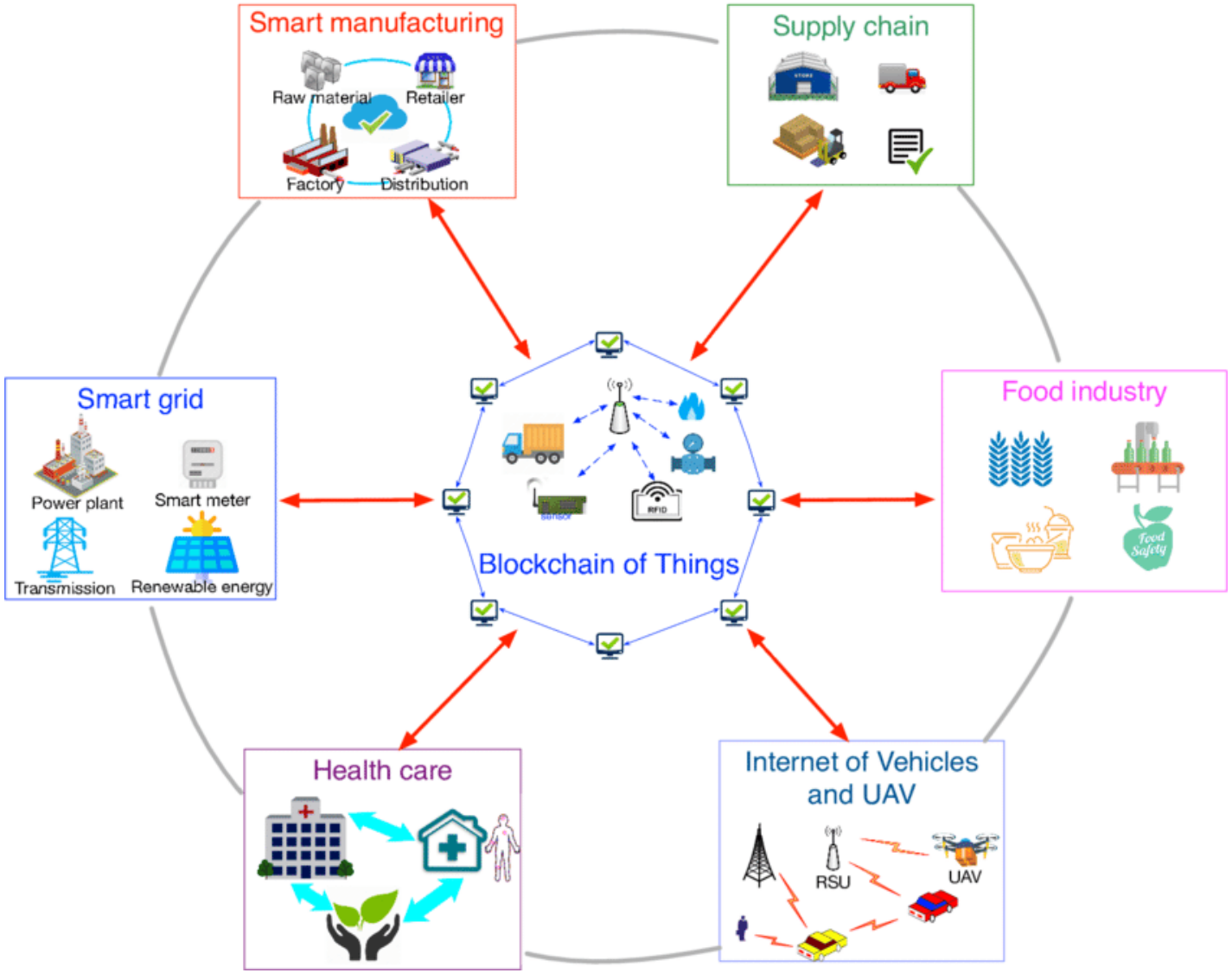
•Pythonic programming language.
•Strong typing.
•Small and understandable compiler code.
•Efficient bytecode generation.
•Deliberately has less features than Solidity with the aim of making contracts more secure and easier to audit. Vyper does **not** support:

- Modifiers
- Inheritance
- Inline assembly
- Function overloading
- Operator overloading
- Recursive calling
- Infinite-length loops
- Binary fixed points

Part 2.

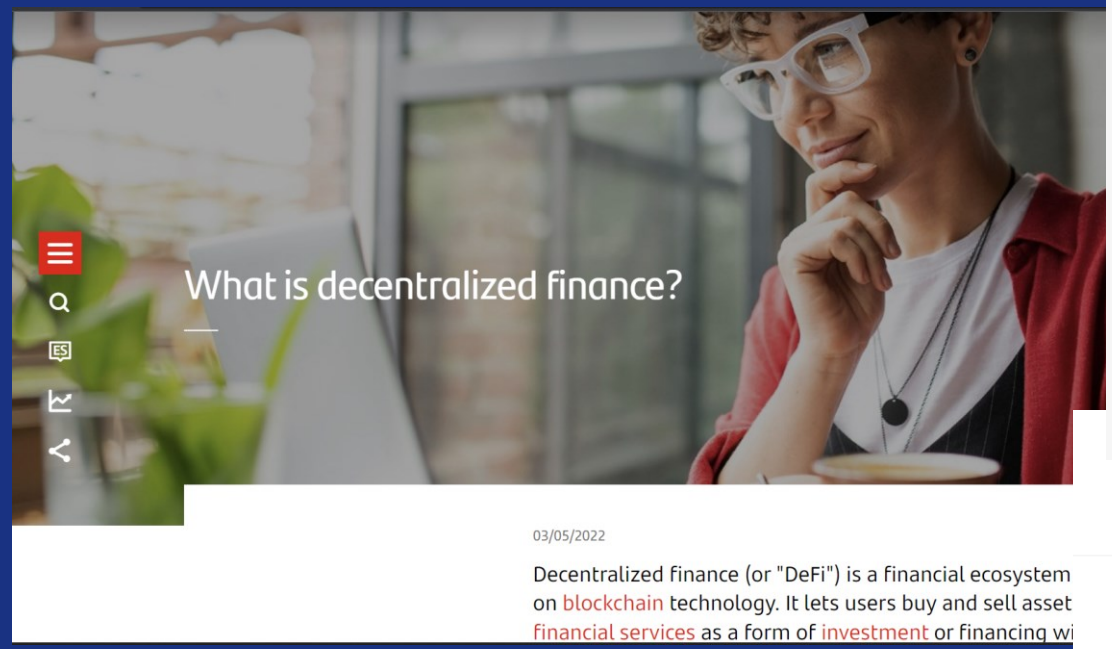
Blockchain use cases and applications

IoT



Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076-8094.

DeFI (DECENTRALIZED FINANCE)



ONYX by J.P.Morgan

About Onyx | Our Offerings | Learn | Contact Us

Institutional DeFi

The Next Generation of Finance

We believe a version of decentralized finance (DeFi) called "Institutional DeFi", which combines the innovations of DeFi protocols with the safeguards of today's finance industry, has the potential for growth and transformative impact.

The aim of this joint report by the Oliver Wyman Forum, DBS, Onyx by J.P. Morgan, and SBI Digital Asset Holdings is to help business executives understand the potential benefits of adapting decentralized finance (DeFi) protocols in the finance industry using tokenized real-world assets.

This paper explains what industry participants need to do to achieve regulatory clarity, drive commercial adoption, and get the greatest benefits out of Institutional DeFi for their clients and themselves.

Read the report →

BBVA

INNOVATION | FINANCE | ECONOMY | SUSTAINABILITY AND RESPONSIBLE BANKING | OPENMIND | PODCAST | CENYT CASE

BLOCKCHAIN | 05 Jul 2021

Decentralized finance is on the rise

Decentralized finance is a blockchain-based set of applications that, in principle, need no intermediaries to work. These financial products have similar characteristics to traditional services and their boom period could, to some extent, change the financial sector and give rise to both opportunities and challenges.

DeFI (DECENTRALIZED FINANCE)

- Financial products with features similar to traditional services, but created within a blockchain
- Open-source protocols capable of issuing assets, processing transactions, and facilitating financial agreements.
- Use of smart contracts for monetary transactions.
- Difference from traditional finance: no bank account is needed, only internet access or a digital wallet.

DeFI - BENEFITS

- Autonomy and Control.
- Decentralization and Censorship Resistance.
- Efficiency and Security.
- Transparency and Resilience.

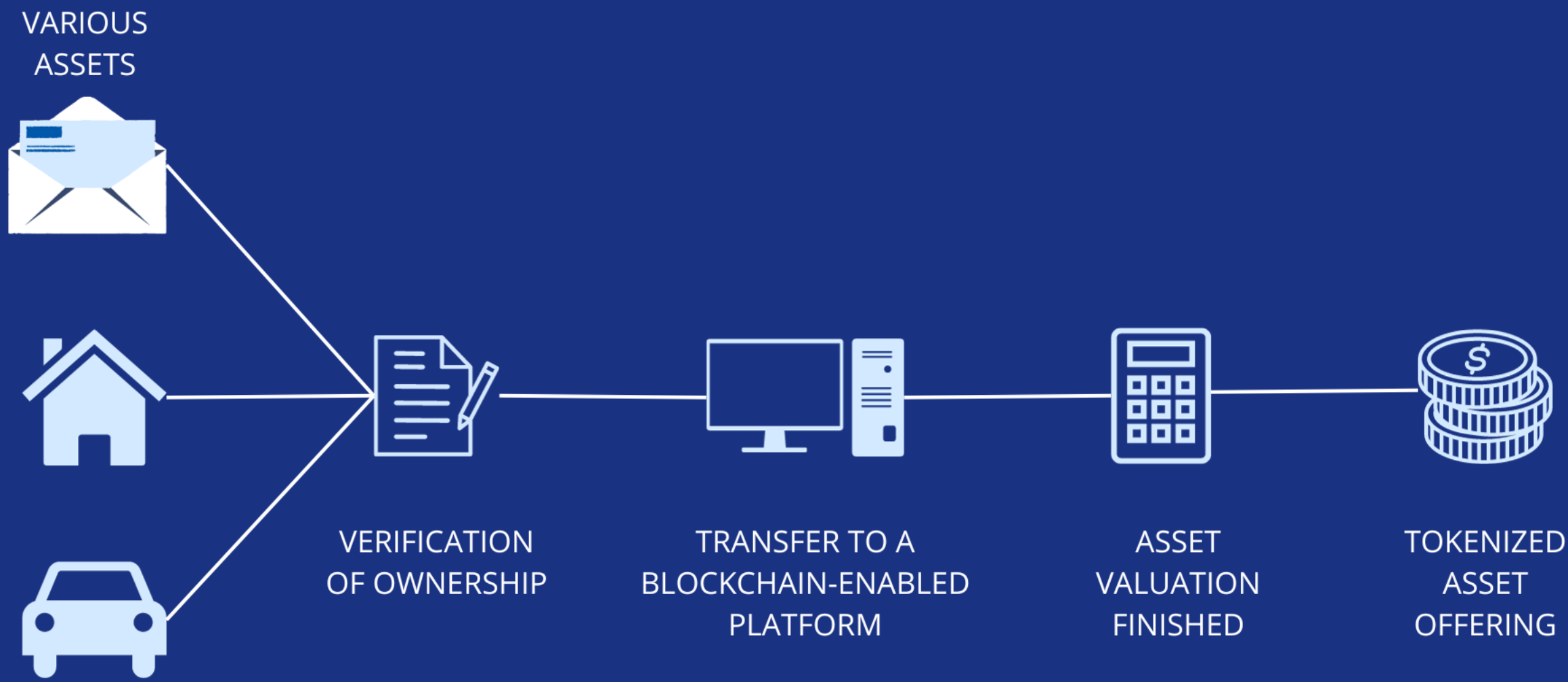
TOKENIZATION

- Cryptographic assets that do not have their own blockchain.
- They have secondary markets that depend on the value of their utility.
- Commonly created by companies, organizations, or individuals.
- Multiple use cases (especially in DeFi).

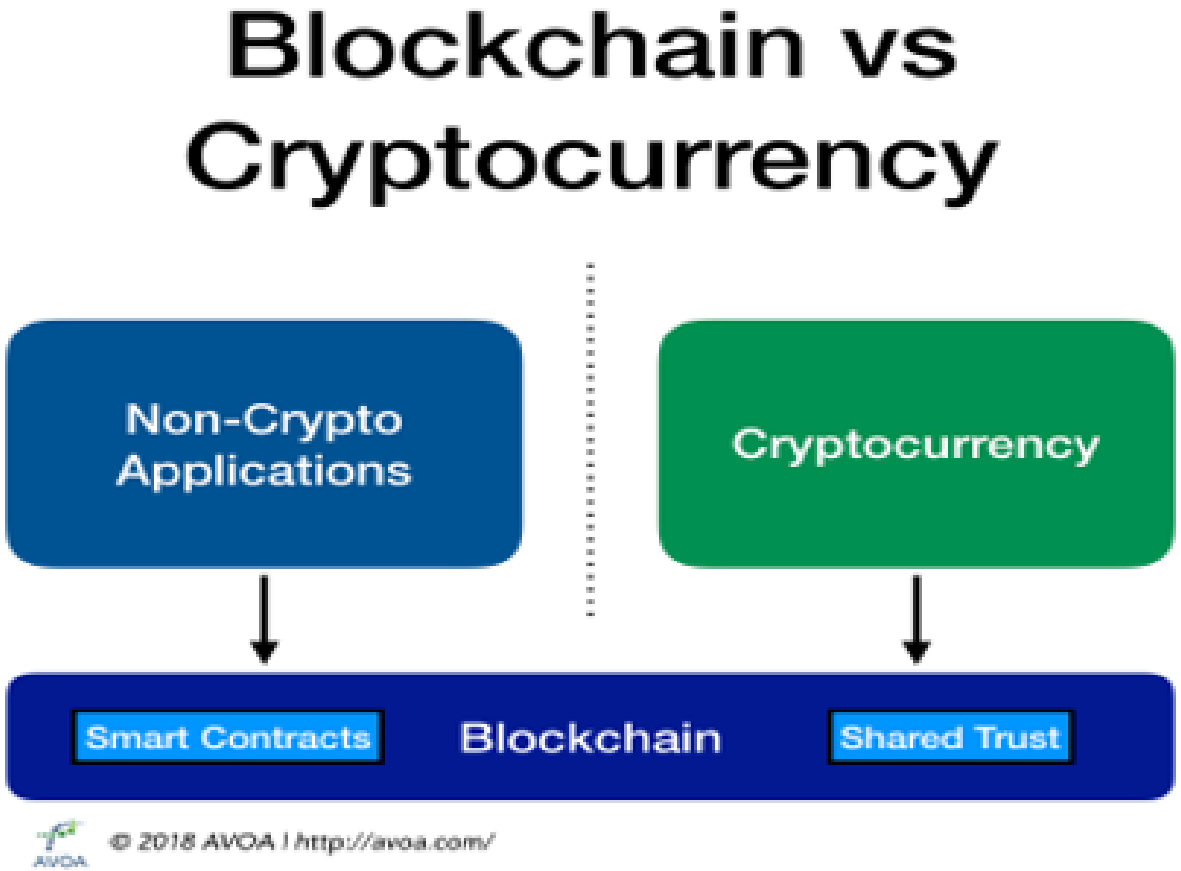
TOKENIZATION IN REAL STATE

- Real estate tokenization is a process involving the conversion of real property into digital tokens.
- These tokens can be bought, sold, and traded on a blockchain platform.
- Benefits: increased liquidity, transparency, and accessibility for investors.

TOKENIZATION PROCESS



Difference between blockchain and bitcoin



Part 3.

Creating our own Blockchain network

Existing blockchain platforms

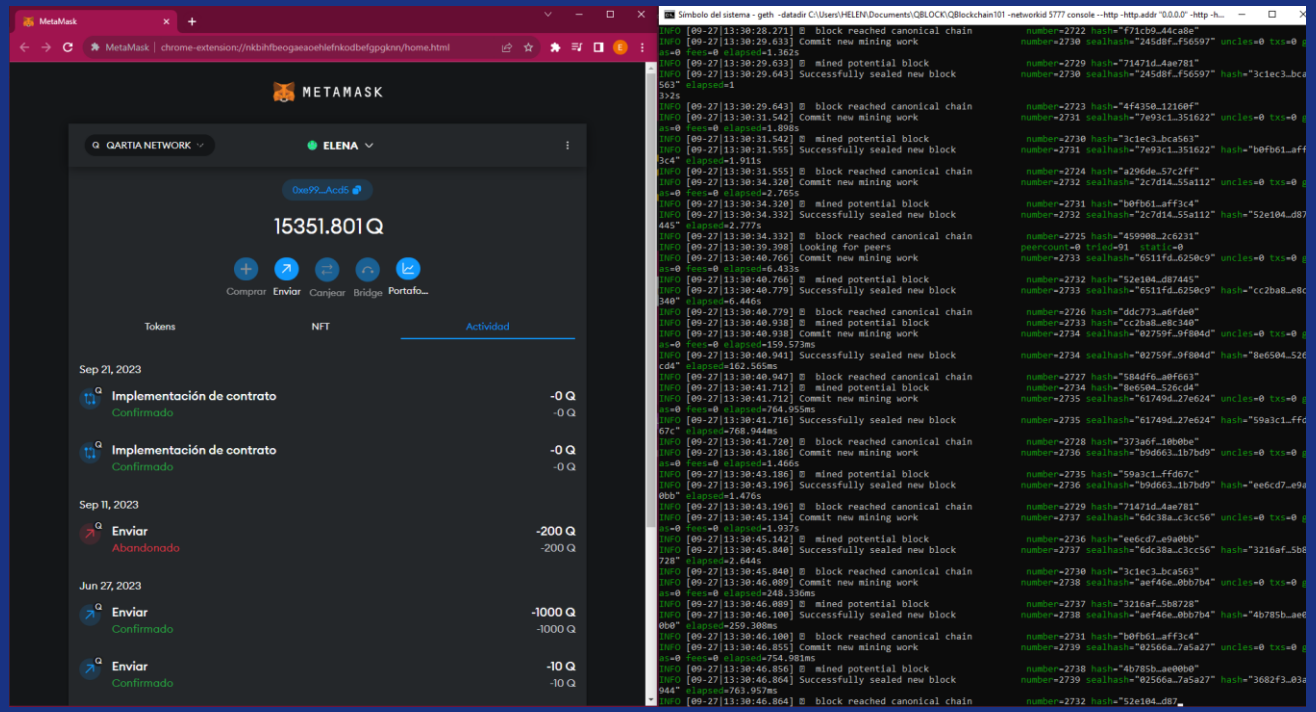
Platform	Blockchain	Popularity & Active	Consensus Algorithm	Pricing	Supported Languages	Smart Contracts
Bitcoin	Public	High	PoW	Fees per transaction	Script and C++	No
Ethereum	Public and permissioned	High	PoW, PoS GHOST	Ether for translation and computational service	Python, Go, C++, Java Scripts	Yes
Hyberledeger-Fabric	Private, Permissioned	High	PBTF	Open Source price	Python, Golang and Java	Yes
Multichain	Private, Permissioned	Medium	PBTF	Free, Open Source price	Python, C#, JavaScript, PHP, Ruby	Yes
Quorum	Public, Permissioned	High	Raft, IBFT	Fees per transaction	Python, Go, C++, Java Scripts	Yes
Lisk	Public and permissioned	Medium	DPoS	Fees per transaction	JavaScript	Yes
LiteCoin	Public	Low	Scrypt	Fees per transaction	C++	No
HDAC	Public and permissioned	Low	EPoW	Fees per transaction	Web Assembly	Yes
IOTA	Public, Permissioned	Low	PoW, TANGLE	Pricing not clear as yet	Python, C, JavaScript	No

Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S. A., & Karim, F. K. (2022). Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions. *Electronics*, *11*(4), 630.

TECHNOLOGIES USED

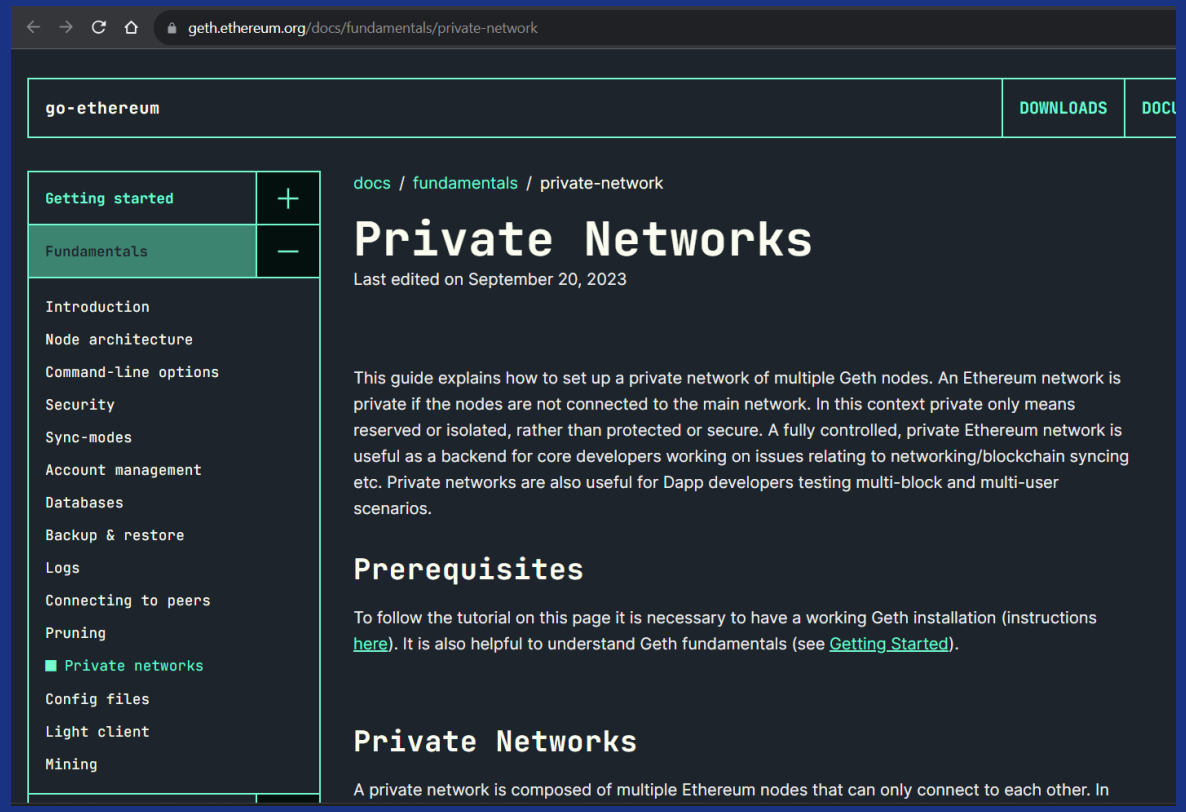
- Built our Blockchain using a framework called Truffle Suite, based on Ethereum technology and programmed in languages like Solidity and JavaScript.
- The data we use is processed with Telegraf and collected in an InfluxDB database.
- Additionally, we use the block generator Geth connected to our wallet and our Truffle Suite to run our Blockchain.

OUR OWN PRIVATE BLOCKCHAIN



Our own Ethereum-based Blockchain network, creating a secure environment tailored to our specific needs, such us our own currency, data validation, and transactions.

OUR OWN PRIVATE BLOCKCHAIN



- Ethereum Node.
- Open-Source.
- Supports Ethereum Network.
- Block Generator.
- Used for Private Networks.

OUR OWN PRIVATE BLOCKCHAIN

```
{
  "config": {
    "chainId": 12345,
    "homesteadBlock": 0,
    "eip150Block": 0,
    "eip155Block": 0,
    "eip158Block": 0,
    "byzantiumBlock": 0,
    "constantinopleBlock": 0,
    "petersburgBlock": 0,
    "istanbulBlock": 0,
    "berlinBlock": 0,
    "ethash": {}
  },
  "difficulty": "1",
  "gasLimit": "8000000",
  "alloc": {
    "7df9a875a174b3bc565e6424a0050ebc1b2d1d82": { "balance": "300000" },
    "f41c74c9ae680c1aa78f42e5647a62f353b7bdde": { "balance": "400000" }
  }
}
```

- Creation of our Genesis Block with its own network ID.
- A private group of entities start their blockchain and use it as a permissioned blockchain.

In conclusion

1. *New possibilities for secure, decentralized, and authenticated data management.*
2. *It can help improve data transparency and traceability.*
3. *It can be deployed in various production environments.*
4. *Great potential.*

That’s all!

MINISTERIO DE CIENCIA E INNOVACIÓN
Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
AGENCIA ESTATAL DE INVESTIGACIÓN