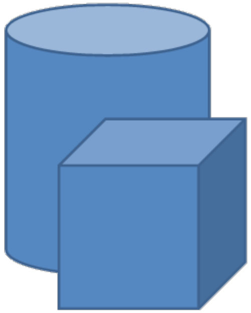
Demystifying

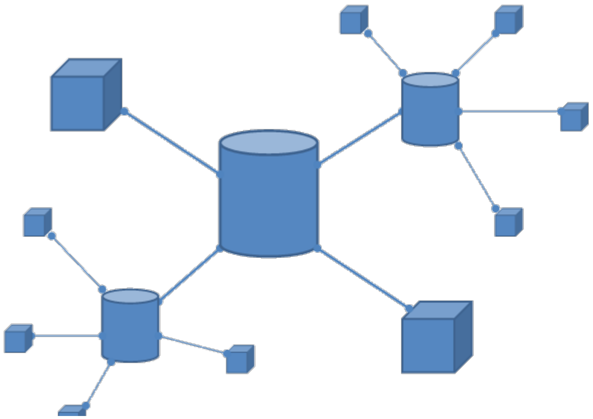
ati

ltant

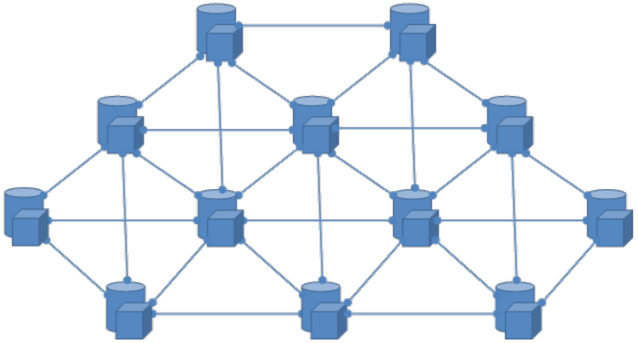
Network Architectures



Centralised

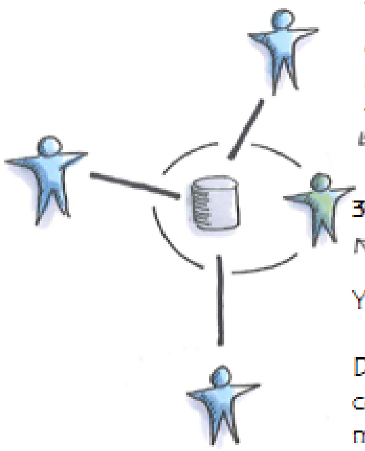


Decentralised



Distributed

Centralised



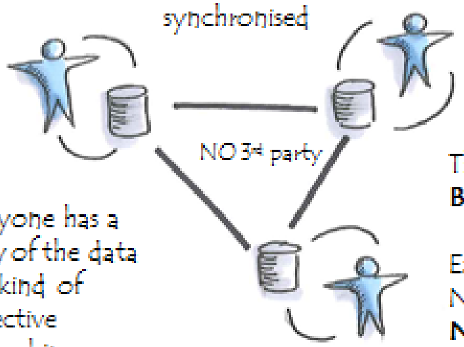
This guy owns the data and will likely charge you to see it

3rd Party

You have to trust him!

Data can be compromised due to mistakes or to serve the 3rd party's purpose

Distributed



Blockchain keeps all of the data synchronised

NO 3rd party

Everyone has a copy of the data in a kind of collective ownership

This is called a **Blockchain Network**

Each party in the Network is called a **Node**

The trust has allowed a handful of companies (GAFAM) to centralize data from a huge part of the population, holding a near-monopoly on our digital lives.

The **dangers and stakes** are threefold: **economic, technological, cultural.**

What is at stake?

Surveillance

Privacy

Centralization

Termination

10 Biggest Data Breaches of 2018

Aadhaar

- 1.1 billion records breached
- Date disclosed: January 3, 2018

Exactis

- 340 million records breached
- Date disclosed: June 26, 2018

Under Armour

- 150 million records breached
- Date disclosed: May 25, 2018

MyHeritage

- 92 million records breached
- Date disclosed: June 4, 2018

Facebook

- 87 million records breached
- Date disclosed: March 17, 2018

Panera

- 37 million records breached
- Date disclosed: April 2, 2018

Ticketfly

- 27 million records breached
- Date disclosed: June 7, 2018

Sacramento Bee

- 19.5 million records breached
- Date disclosed: June 7, 2018

PumpUp

- 6 million records breached
- Date disclosed: May 31, 2018

Saks, Lord & Taylor

- 5 million records breached
- Date disclosed: April 3, 2018

TekMonks

Source : https://blog.barkly.com/biggest-data-breaches-2018-so-far

Any Solution ?

One major factor attributed to the increasing number of fraudulent activities is due to the use of **centralized servers.**

Possible Solution

“We can **adopt a decentralized** approach”

Don TapScott, an academic and businessman, and author of messianic book , has called blockchain technology “**the trust protocol**”.

“You **don’t need intermediaries to ensure parties** will act with integrity, because the very platform you’re transacting on does that for you,” he says.

“**Trust is not achieved by middlemen but by cryptography, collaboration and clever code.**”

Blockchain

“The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.”

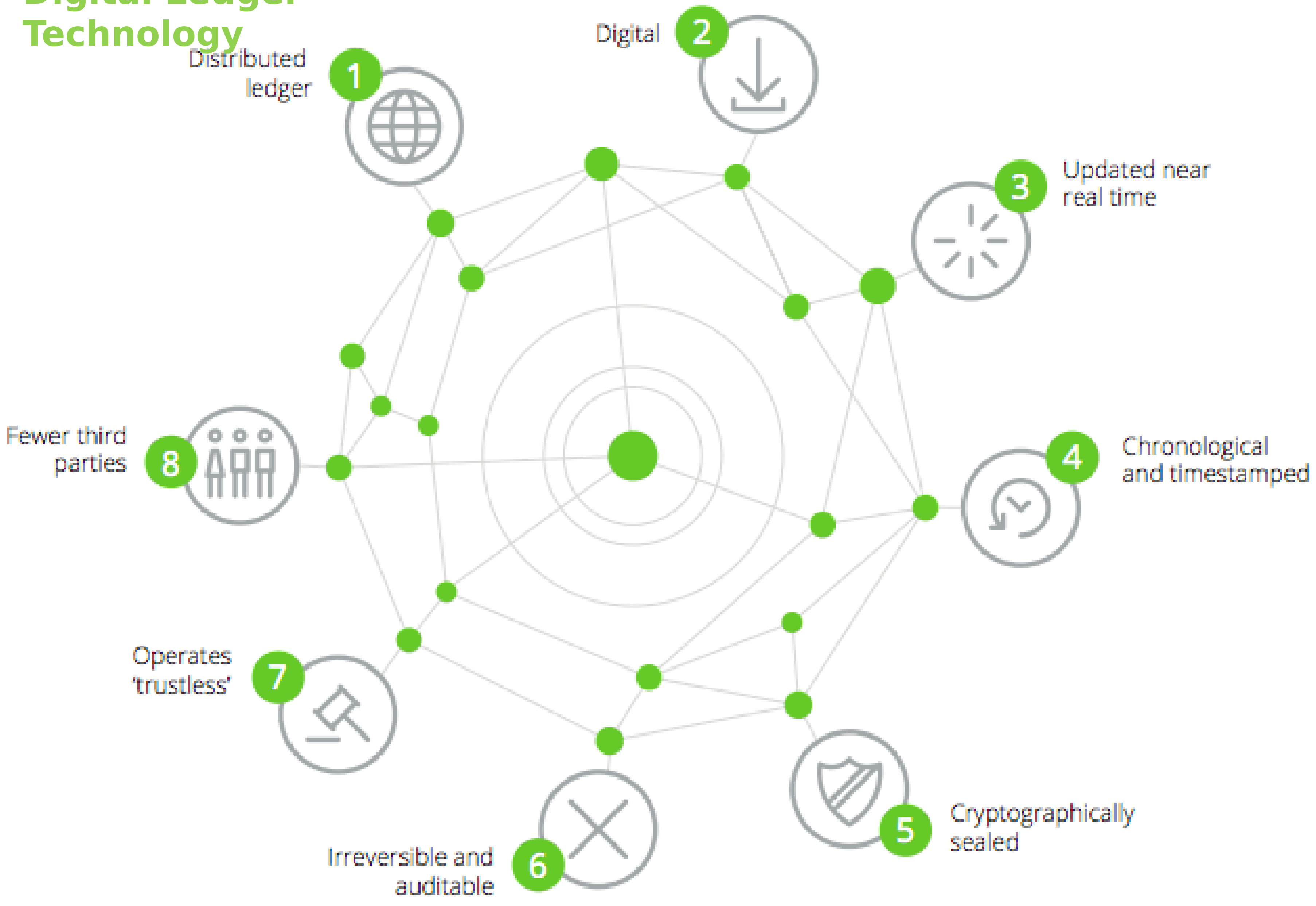
“Blockchain solves the problem of manipulation.

In the West, people say they trust **Google, Facebook, or their banks.**

But the **rest of the world doesn’t trust organizations and corporations** that much — like Africa, India, the Eastern Europe, or Russia.

It’s not about the places where people are really rich. Blockchain’s opportunities are the highest in the countries that haven’t reached that level yet.”

Digital Ledger Technology



Potential benefits of blockchain

Reduce costs of overall transactions

Irrevocable and tamper-resistant transactions

Improved security and efficiency of transactions

Reduction in systemic risks

Fraud minimisation

Enabling effective monitoring and auditing by participants, supervisors, and regulators

Why Blockchain matters?

Enhanced Traceability

Comes in handy when tracking goods in the supply chain.

Increases Trust and Security

No transaction will go through without common consensus of those on the network. All parties are provided secure access to all the information.

Reduces Costs and saves Time

Processes are streamlined and automatic, hence faster. It also removes the need for a middleman.

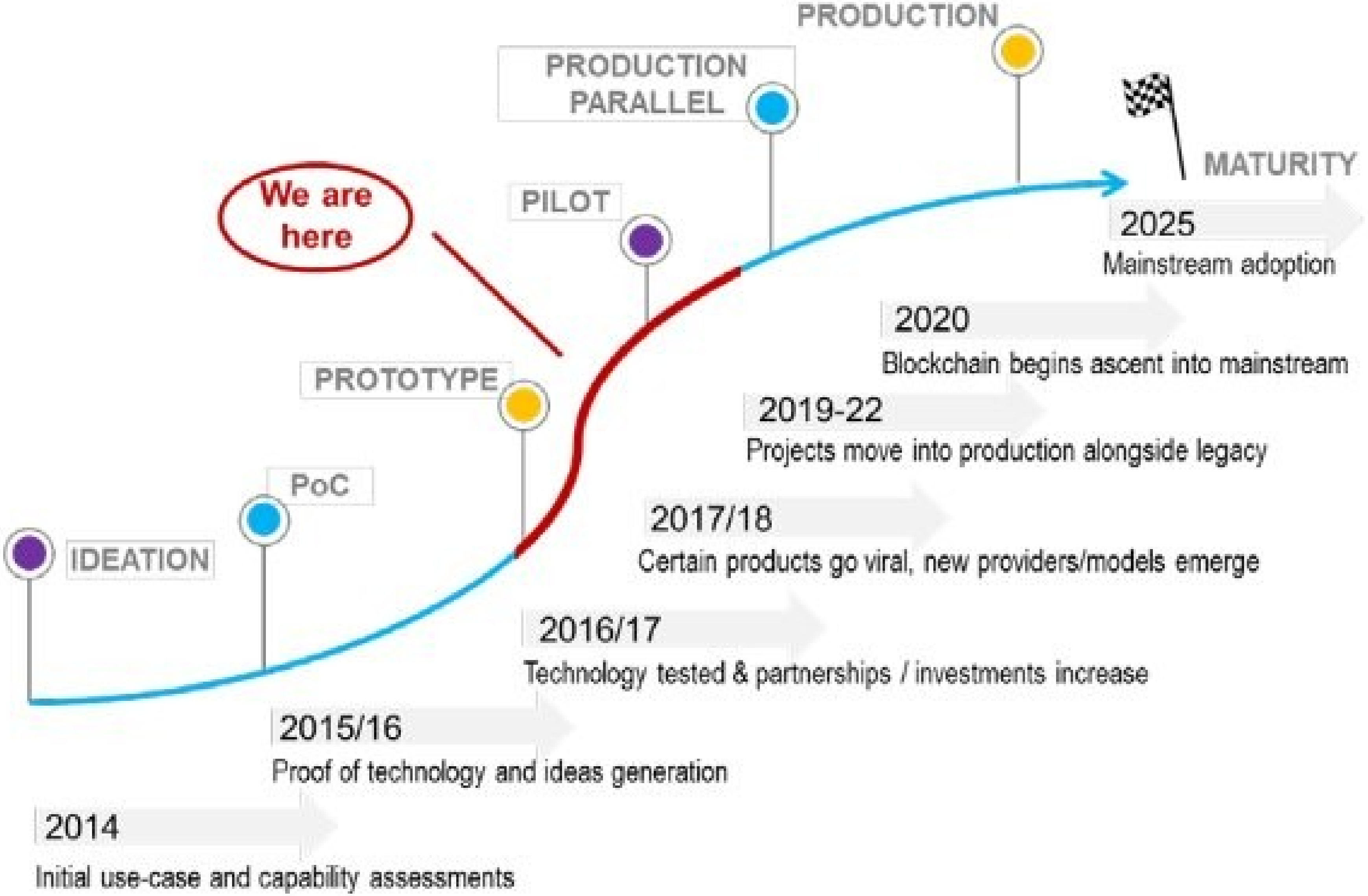
Reduces Risk

Lack of third-party involvement and faster processes, reduces risks for all business types.

Smart Contracts

Contracts that are drawn up between parties in a given network are adhered to automatically. These smart contracts are embedded within the blockchain.

BLOCKCHAIN
HYPE OR HOPE?



2025
Mainstream adoption

2020
Blockchain begins ascent into mainstream

2019-22
Projects move into production alongside legacy

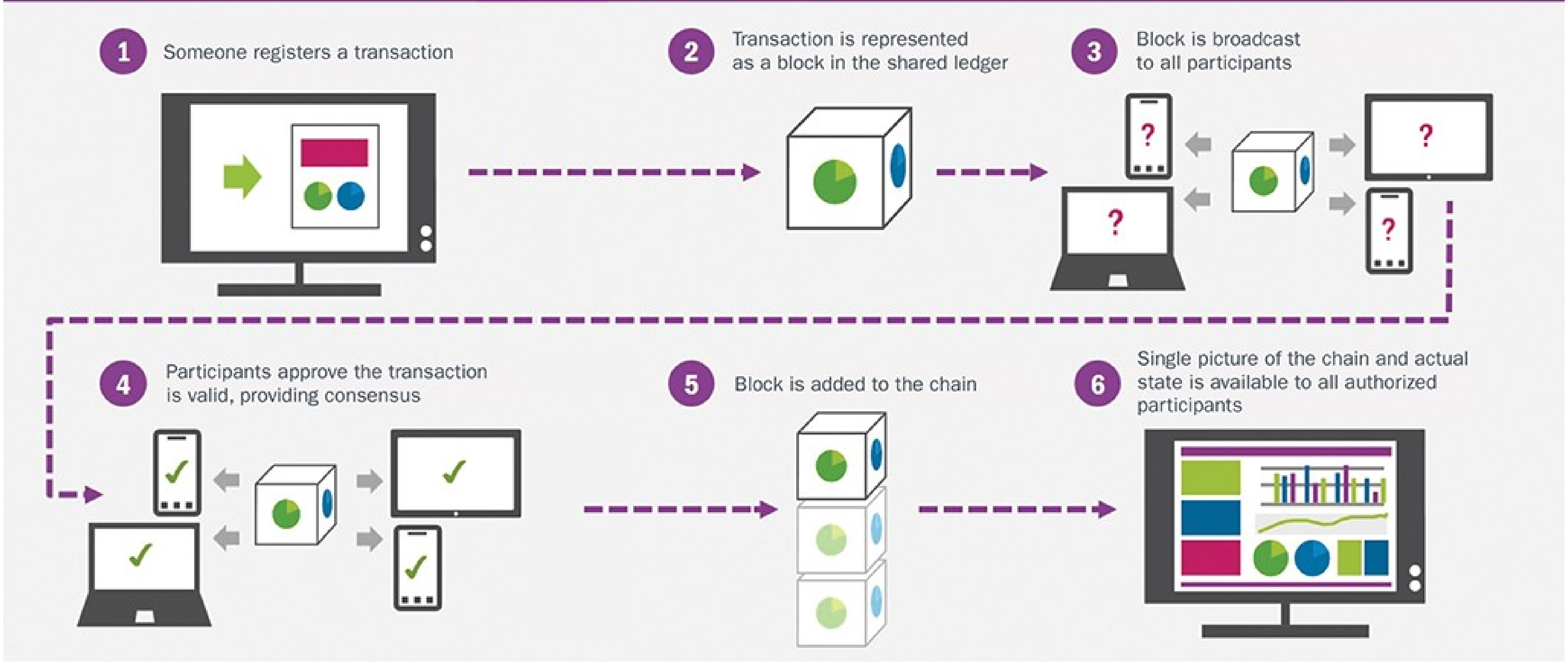
2017/18
Certain products go viral, new providers/models emerge

2016/17
Technology tested & partnerships / investments increase

2015/16
Proof of technology and ideas generation

2014
Initial use-case and capability assessments

HOW BLOCKCHAIN WORKS



1 Someone registers a transaction

2 Transaction is represented as a block in the shared ledger

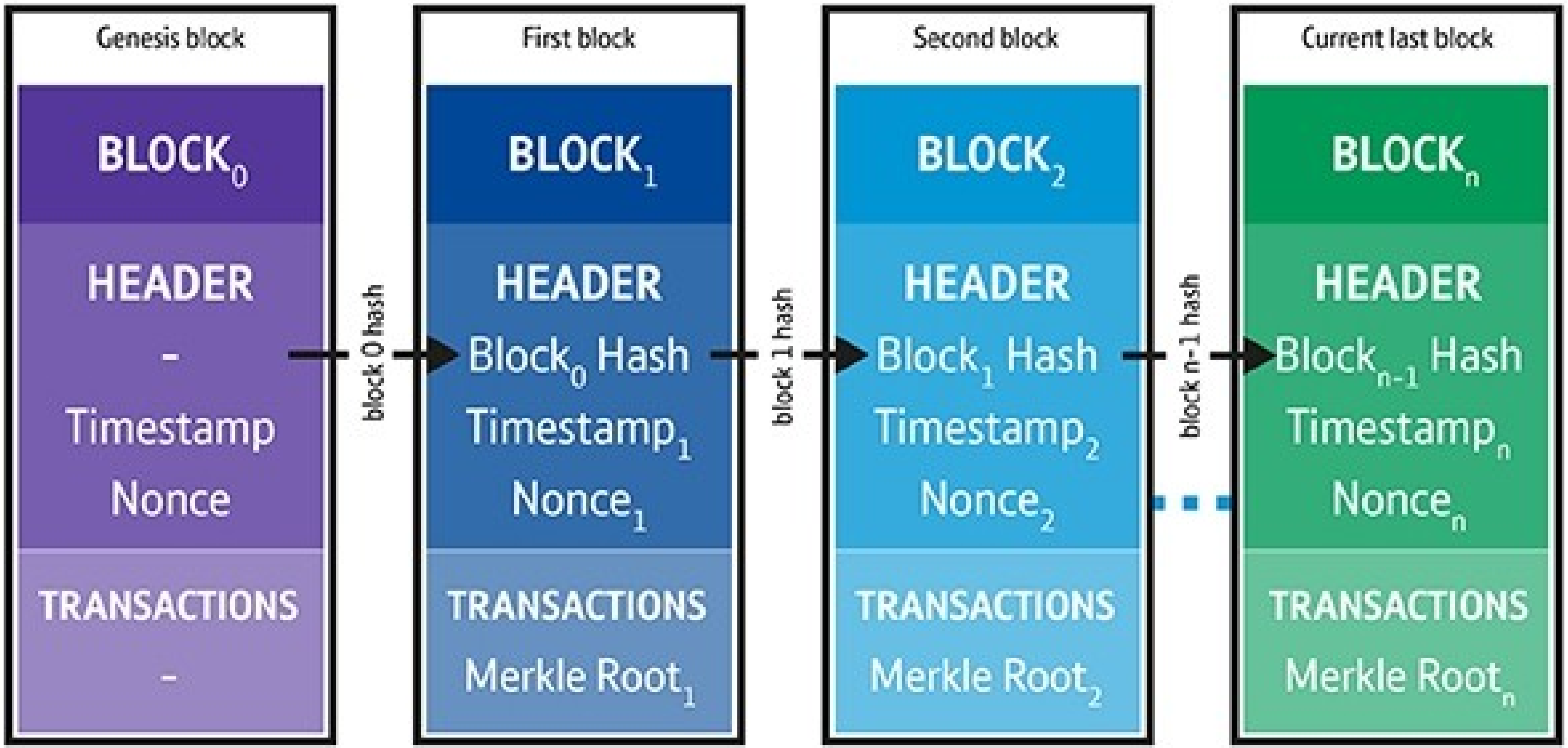
3 Block is broadcast to all participants

4 Participants approve the transaction is valid, providing consensus

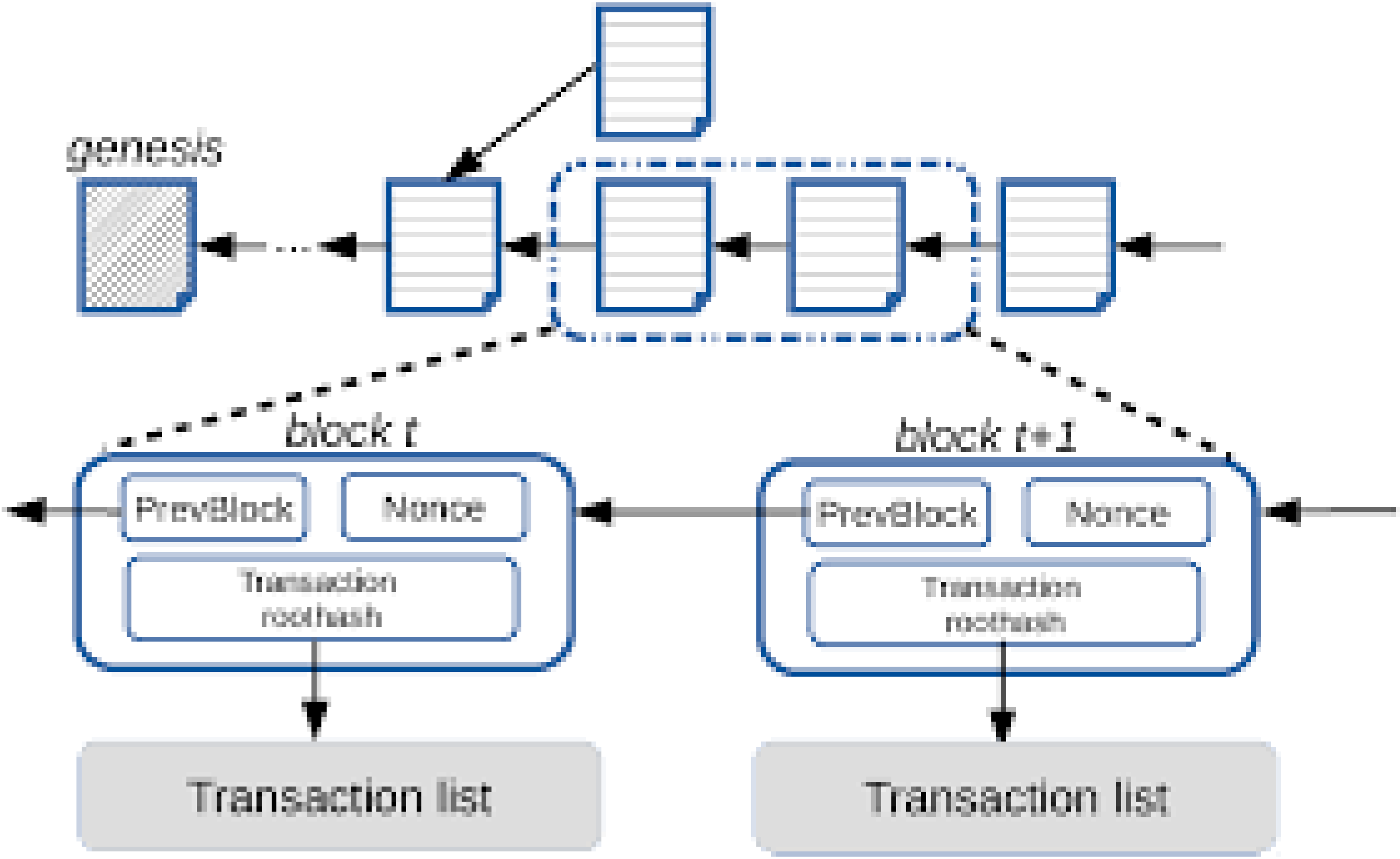
5 Block is added to the chain

6 Single picture of the chain and actual state is available to all authorized participants

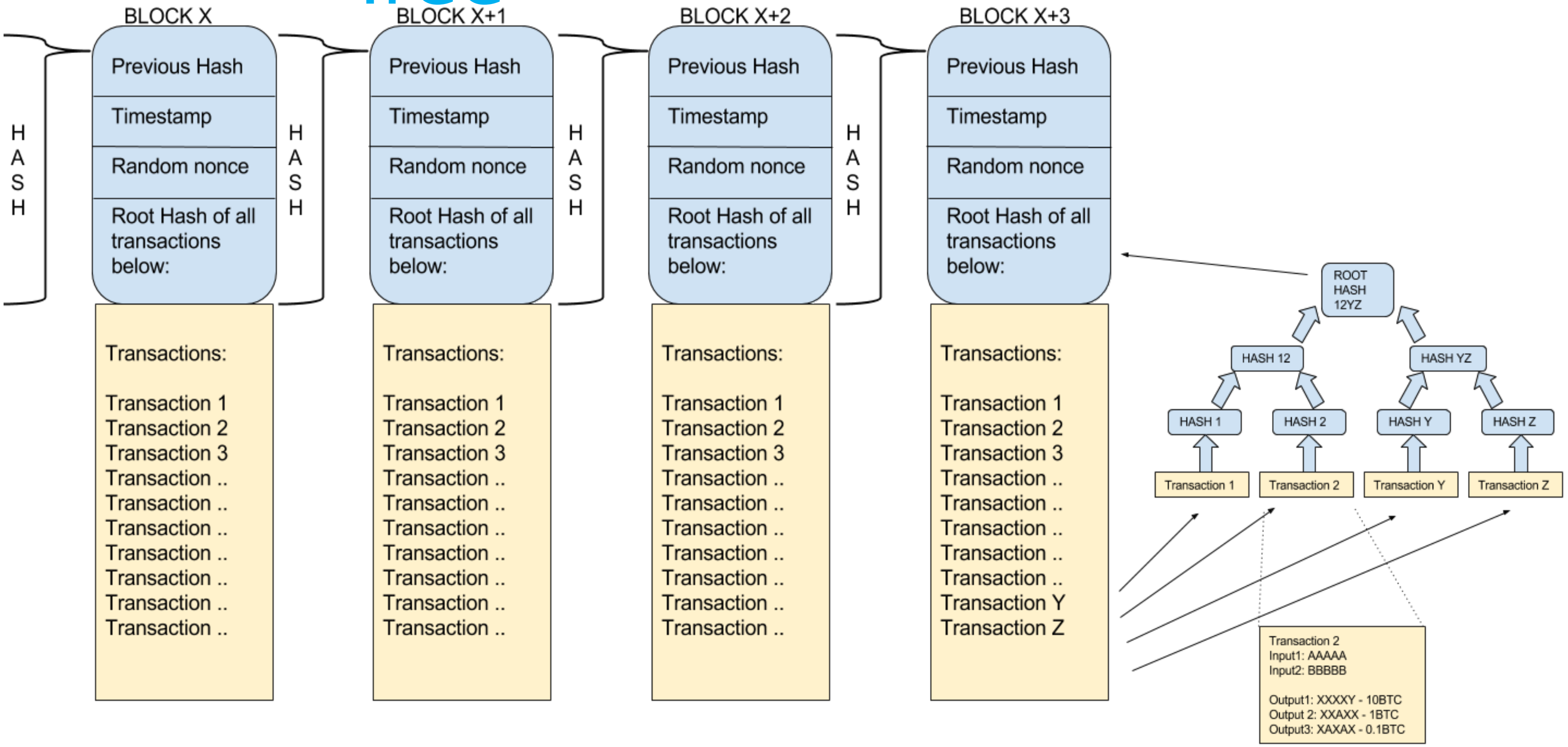
Blocks in Blockchains



Blocks in Blockchain



Blocks and Merkle Tree

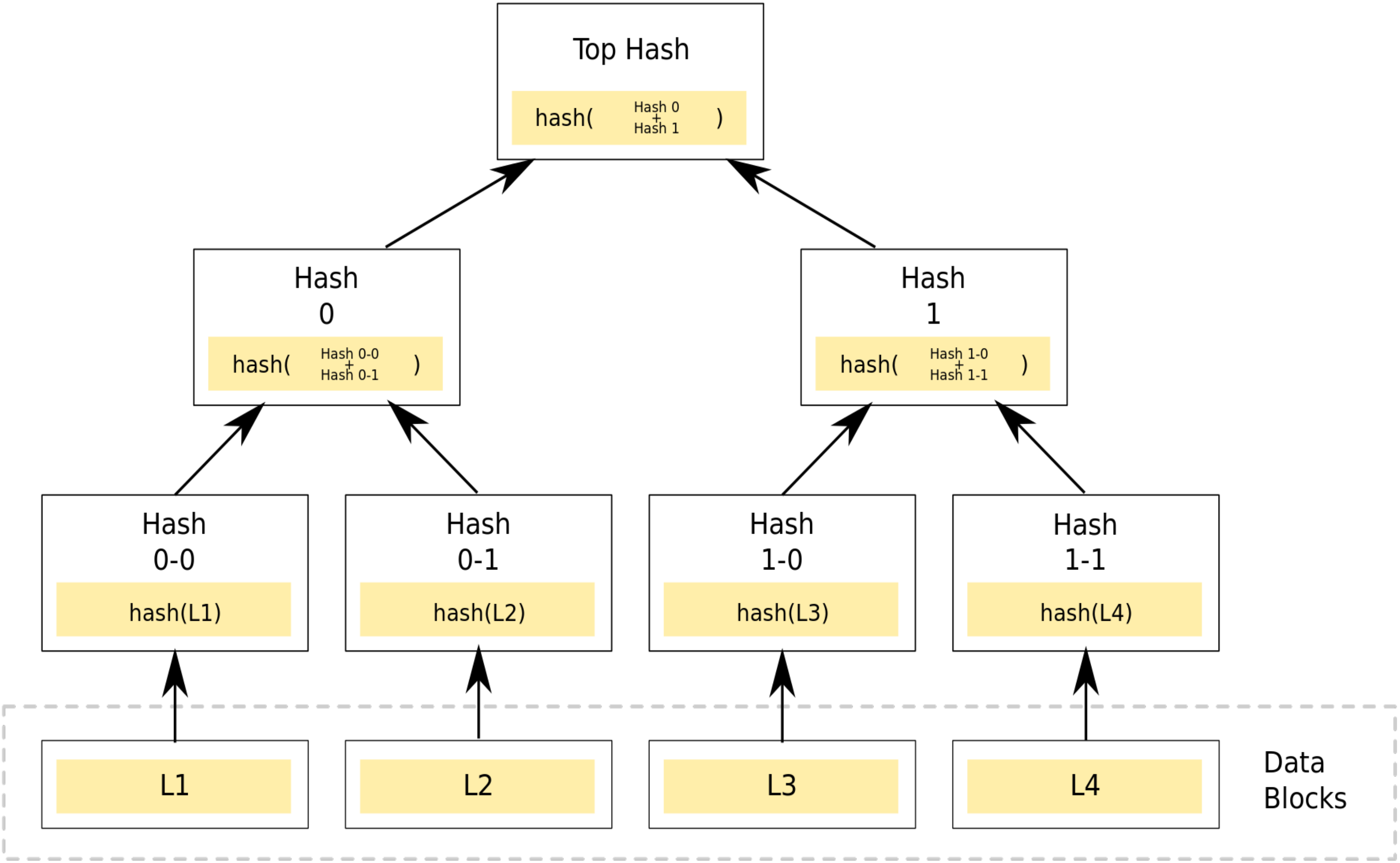


Transaction 2
Input1: AAAAA
Input2: BBBBB

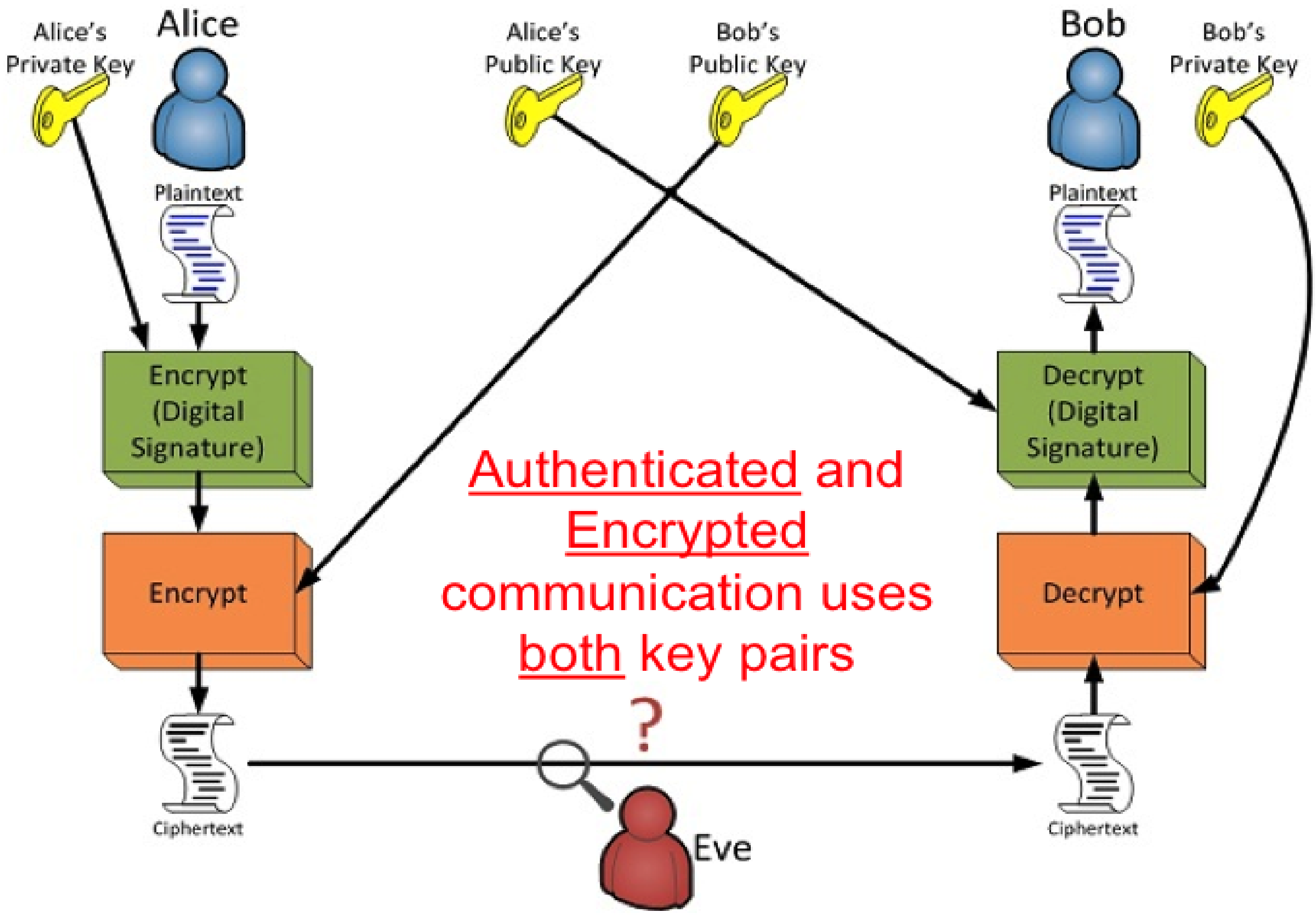
Output1: XXXXY - 10BTC
Output 2: XXAXX - 1BTC
Output3: XAXAX - 0.1BTC

SHA3 – Online Demo : https://emn178.github.io/online-tools/sha3_512.html

Merkle Tree


Top Hash
hash(Hash 0 + Hash 1)
Hash 0
hash(Hash 0-0 + Hash 0-1)
Hash 1
hash(Hash 1-0 + Hash 1-1)
Hash 0-0
hash(L1)
Hash 0-1
hash(L2)
Hash 1-0
hash(L3)
Hash 1-1
hash(L4)
L1
L2
L3
L4
Data Blocks

Public and Private Key

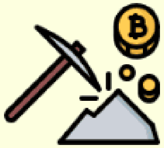
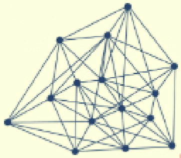
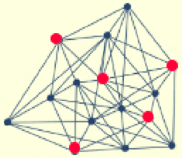
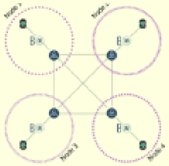
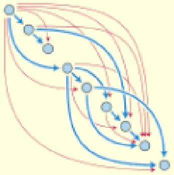


Authenticated and Encrypted communication uses both key pairs

What is **Consensus**

- 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. This often requires processes to agree on some data value that is needed during computation
- A **consensus algorithm** is a process in computer science used to achieve agreement on a single data value among distributed processes or systems.
- **Consensus algorithms** are designed to achieve reliability in a network involving multiple unreliable nodes.

Consensus Algorithms

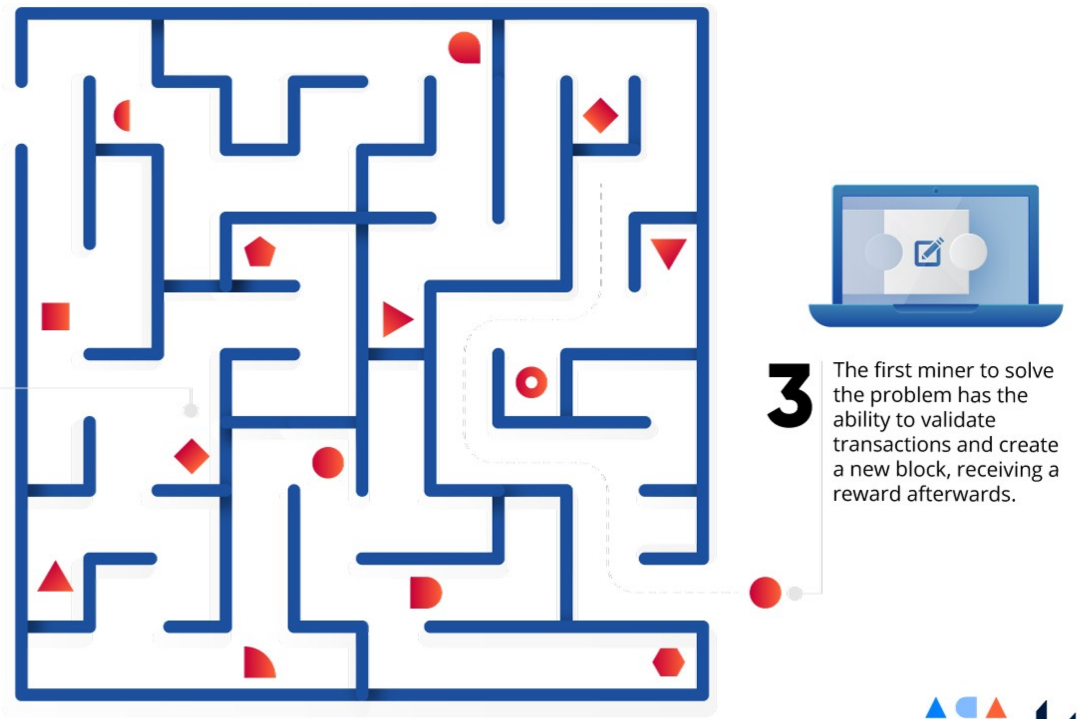
	 Proof-of-Work (POW)	 Proof-of-Stake (POS)	 Delegated Proof-of-Stake (DPOS)	 Byzantine Fault Tolerance	 Directed Acyclic Graphs (DAG)
Energy Consumption	High	Low	Very Low	Very Low	Very Low
Transaction Per Second	7 - 30	30 - 173	2.5 - 2,500	100 - 2,500	180 - 7,000
Transaction Fees	High	Low	Low	Very Low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

Proof of Work

*The system is called **proof of work** because the probability of mining the block is increased with the amount of work that is put in.*

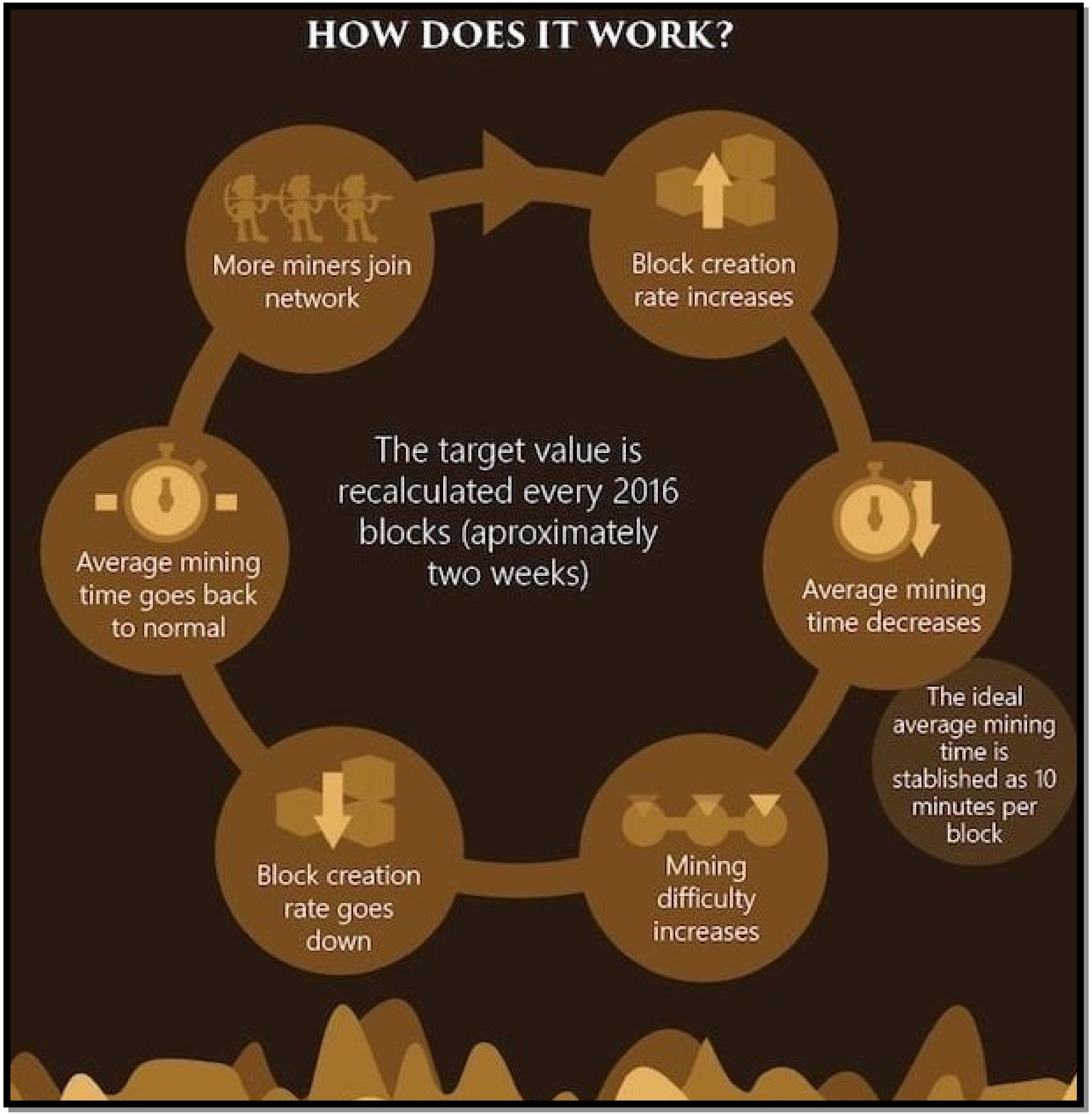
1 A very complex mathematical challenge is proposed to the blockchain network

2 The miners have to compete to find the solution, which takes time and resources, making it costly for the contestants.



3 The first miner to solve the problem has the ability to validate transactions and create a new block, receiving a reward afterwards.

Lisk ACADEMY



HOW DOES IT WORK?

More miners join network

Block creation rate increases

Average mining time decreases

Mining difficulty increases

Block creation rate goes down

Average mining time goes back to normal

The target value is recalculated every 2016 blocks (aproximately two weeks)

The ideal average mining time is stablished as 10 minutes per block

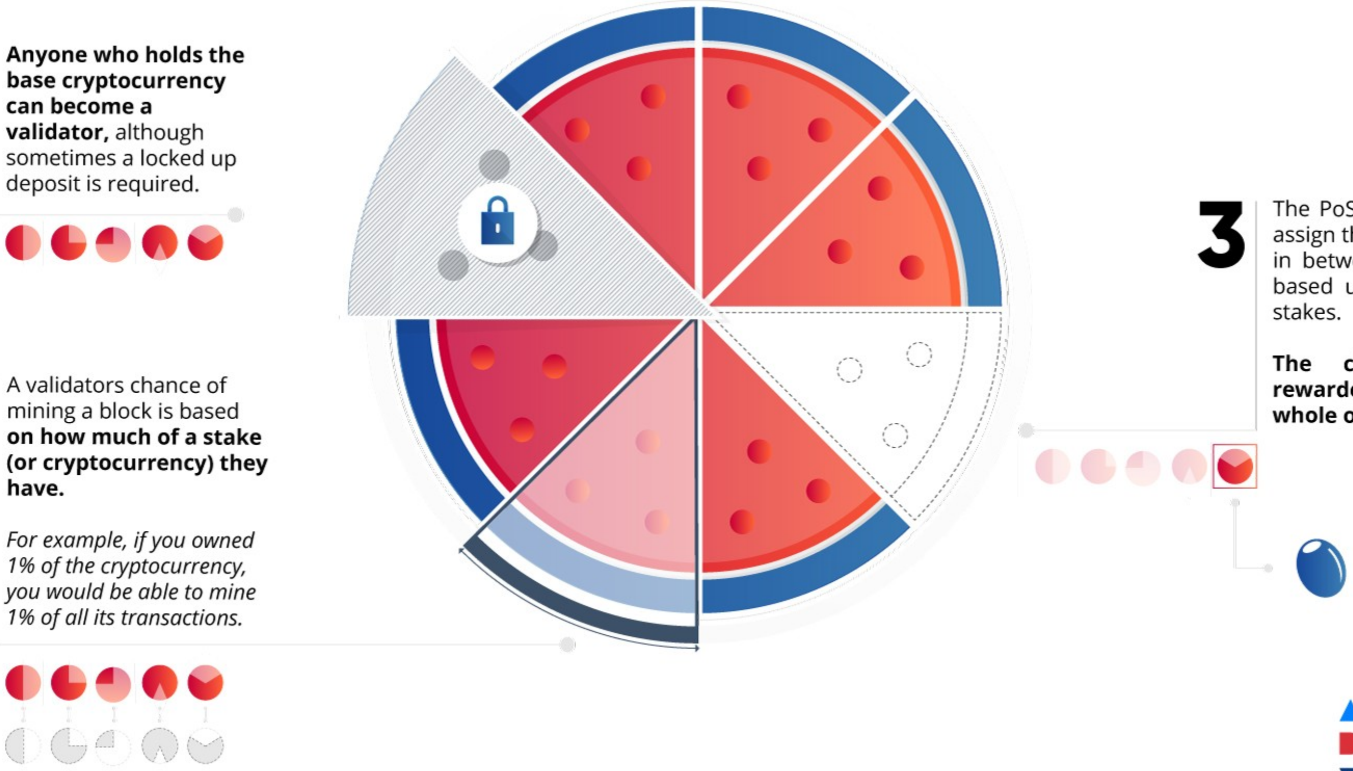
Proof of Stake

*In **Proof of Stake**, each validator owns some stake in the network, and has to lock it in order to be selected.*

1 **Anyone who holds the base cryptocurrency can become a validator,** although sometimes a locked up deposit is required.

2 A validators chance of mining a block is based **on how much of a stake (or cryptocurrency) they have.**

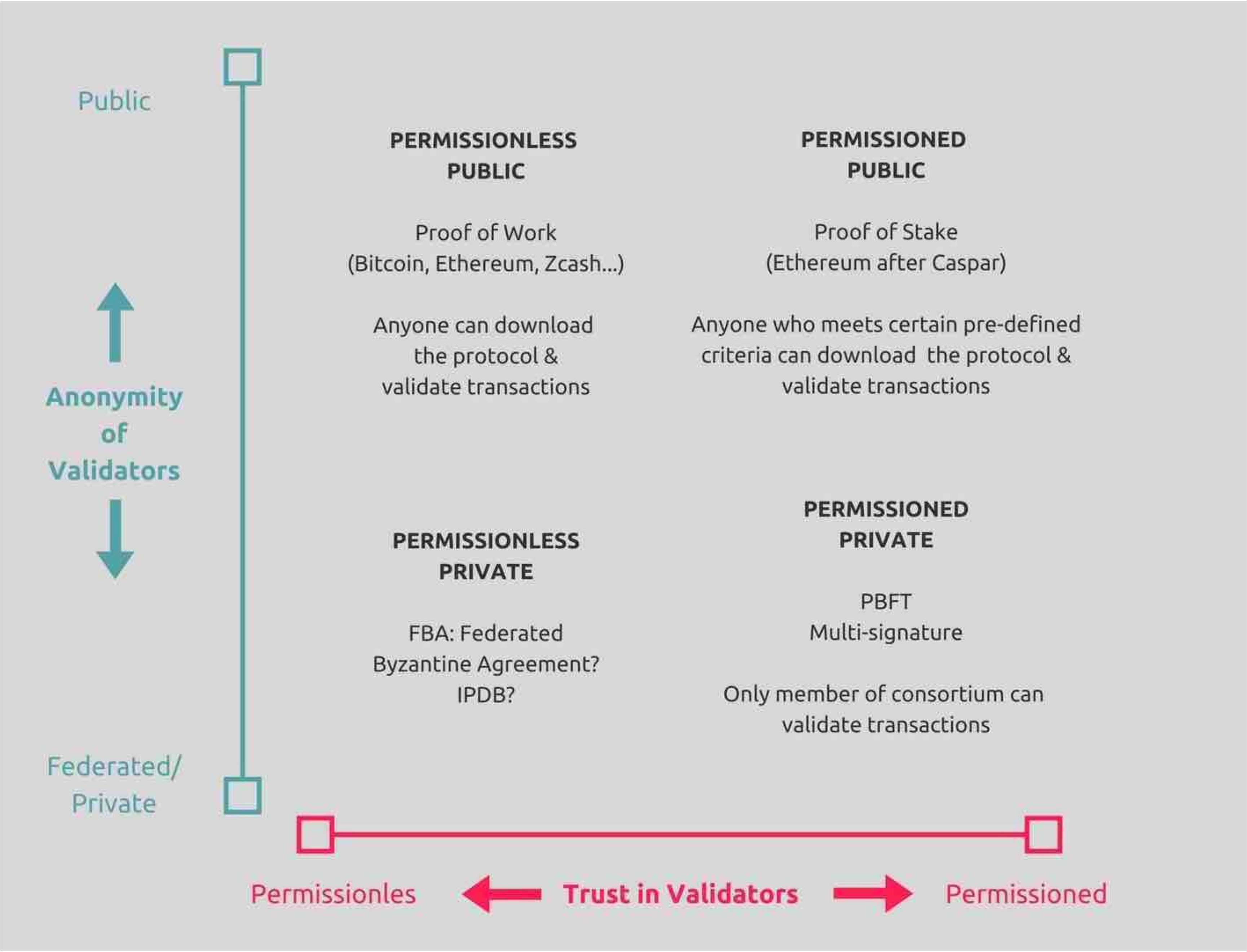
For example, if you owned 1% of the cryptocurrency, you would be able to mine 1% of all its transactions.



3 The PoS protocol will randomly assign the right to create a block in between selected validators, based upon the value of their stakes.

The chosen validator is rewarded by a part or the whole of the transaction fee.

Lisk ACADEMY



Public

Anonymity of Validators

Federated/ Private

PERMISSIONLESS PUBLIC

Proof of Work
(Bitcoin, Ethereum, Zcash...)

Anyone can download the protocol & validate transactions

PERMISSIONED PUBLIC

Proof of Stake
(Ethereum after Caspar)

Anyone who meets certain pre-defined criteria can download the protocol & validate transactions

PERMISSIONLESS PRIVATE

FBA: Federated Byzantine Agreement?
IPDB?

PERMISSIONED PRIVATE

PBFT
Multi-signature

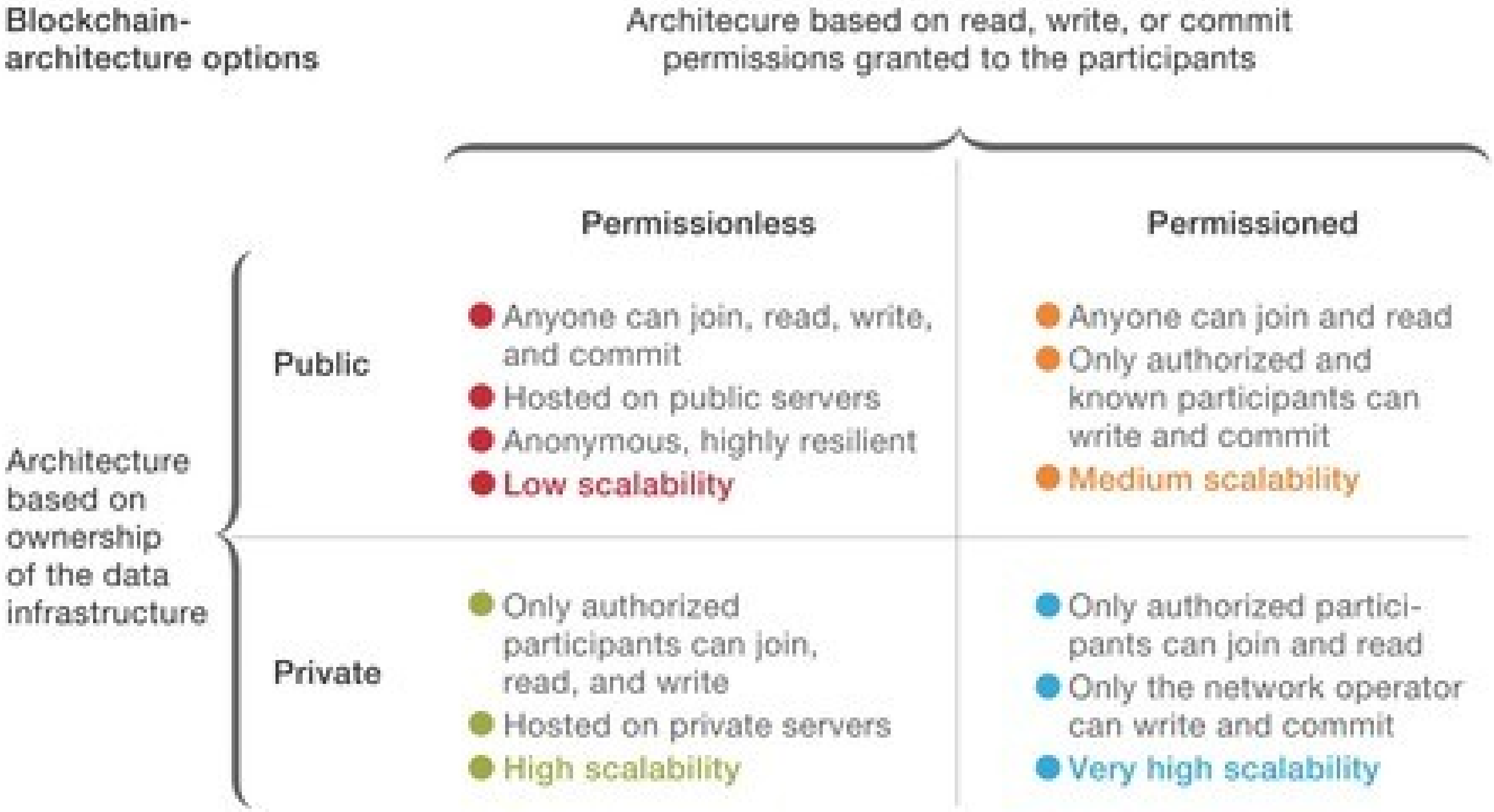
Only member of consortium can validate transactions

Permissionles

Trust in Validators

Permissioned

Most commercial blockchain will use private, permissioned architecture to optimize network openness and scalability.

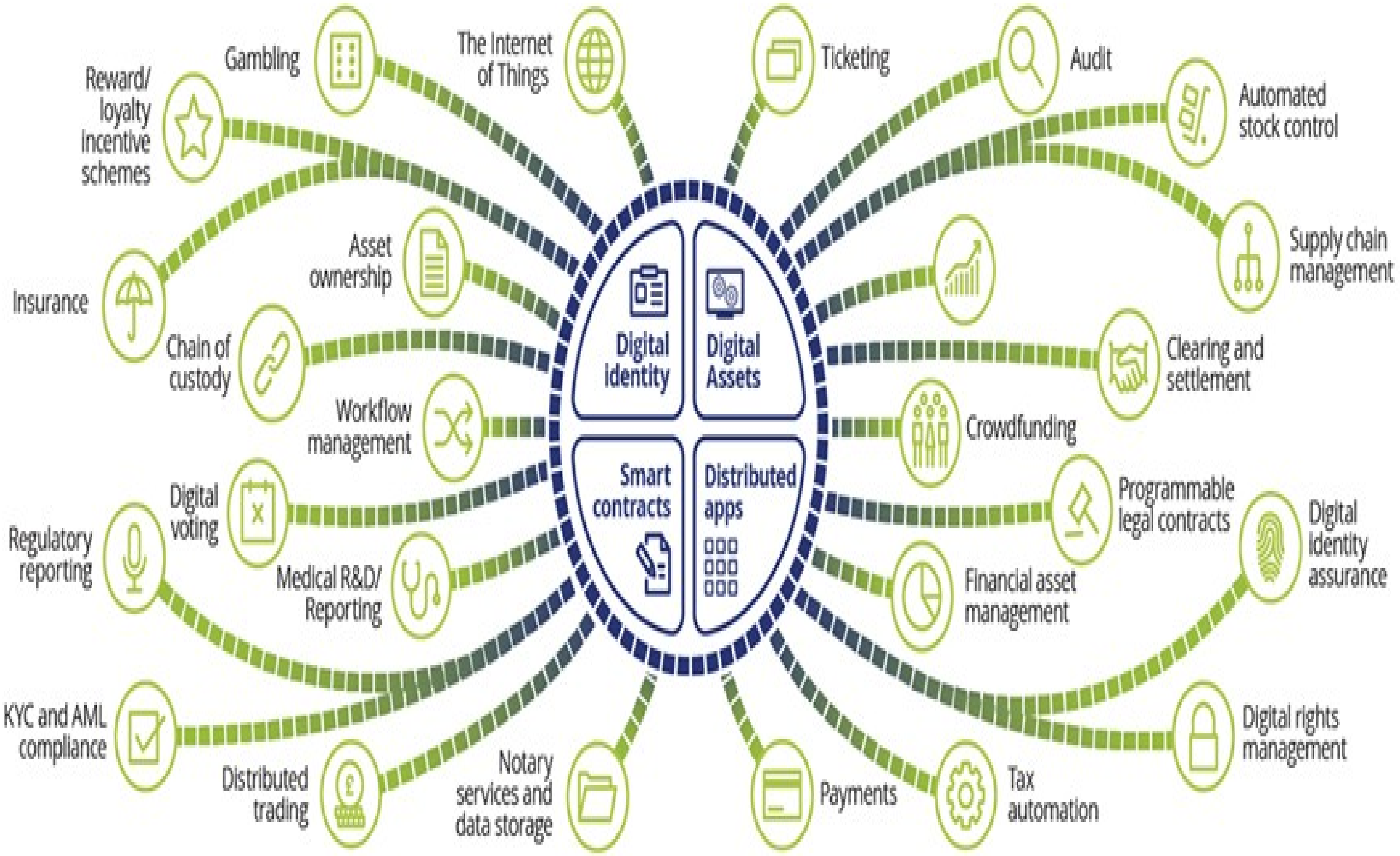


Blockchain-architecture options		Architecure based on read, write, or commit permissions granted to the participants	
		Permissionless	Permissioned
Architecture based on ownership of the data infrastructure	Public	● Anyone can join, read, write, and commit ● Hosted on public servers ● Anonymous, highly resilient ● Low scalability	● Anyone can join and read ● Only authorized and known participants can write and commit ● Medium scalability
	Private	● Only authorized participants can join, read, and write ● Hosted on private servers ● High scalability	● Only authorized participants can join and read ● Only the network operator can write and commit ● Very high scalability

McKinsey&Company

What can you do with a blockchain?

KYC – Know Your Customer
AML – Anti-Money Laundering



SMART CONTRACTS

Traditional contracts	*Smart contracts*
1-3 Days	Minutes
Manual remittance	Automatic remittance
Escrow necessary	Escrow may not be necessary
Expensive	Fraction of the cost
Physical presence (wet signature)	Virtual presence (digital signature)
Lawyers necessary	Lawyers may not be necessary

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.

Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.

Wikipedia

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

Blockgeeks.com

1

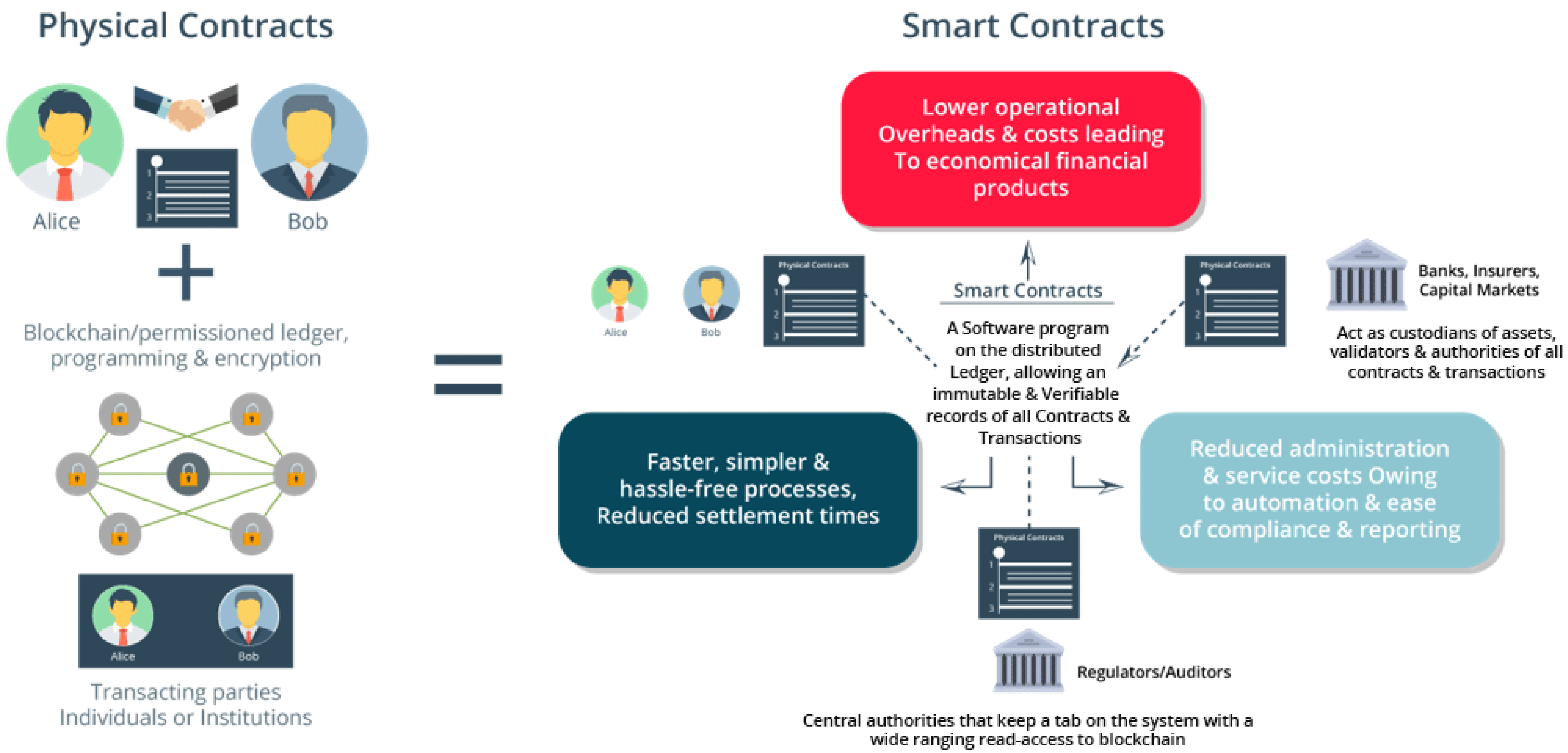
- ✓ A contract is created between two parties
- ✓ Both parties remain anonymous
- ✓ The contract is stored on a public ledger

2

- ✓ Some triggering events are set i.e. deadlines
- ✓ The contract self-executes as per written codes

3

- ✓ Regulators and users can analyze all the activities.
- ✓ Predict market uncertainties and trends



Physical Contracts

+

Blockchain/permissioned ledger, programming & encryption

Transacting parties Individuals or Institutions

=

Smart Contracts

Lower operational Overheads & costs leading To economical financial products

Smart Contracts

A Software program on the distributed Ledger, allowing an immutable & Verifiable records of all Contracts & Transactions

Banks, Insurers, Capital Markets

Act as custodians of assets, validators & authorities of all contracts & transactions

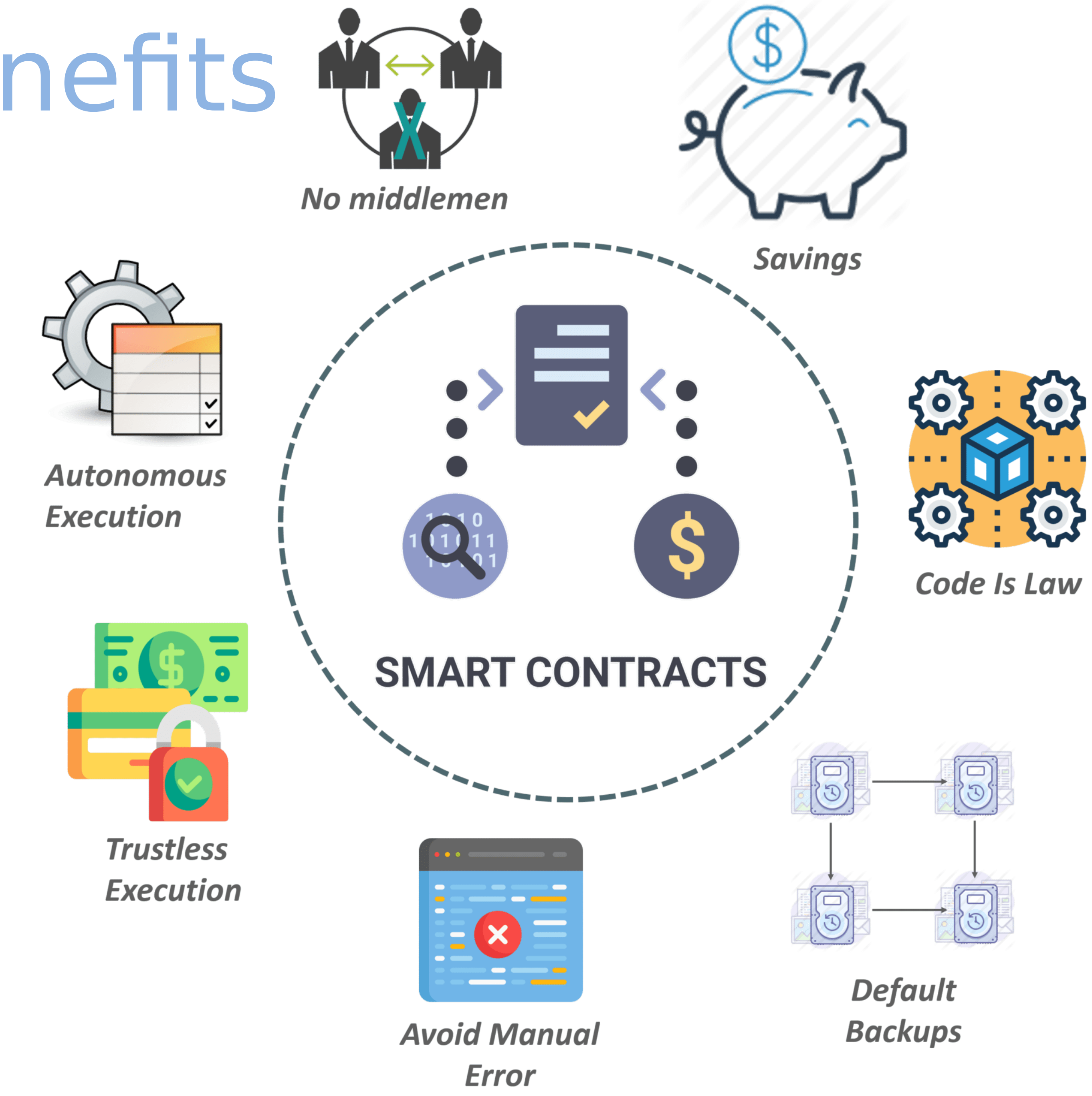
Faster, simpler & hassle-free processes, Reduced settlement times

Reduced administration & service costs Owing to automation & ease of compliance & reporting

Regulators/Auditors

Central authorities that keep a tab on the system with a wide ranging read-access to blockchain

Benefits



SMART CONTRACTS

No middlemen

Savings

Autonomous Execution

Code Is Law

Trustless Execution

Default Backups

Avoid Manual Error