Block Chain Technology

Blockchain basics

Blockchain demo

- Hash
- Block
- Blockchain
- Distributed
- Tokens
- Coinbase

[Source - https://andersbrownworth.com/blockchain]

Your understanding of Blockchain tech

Mentimeter

chain of immutable blocks

linked data structure

accountabiltiy

no central authorityblock

confidentiality

bitcoin

distributed system

integrity

secure transaction

chain of blocks

future

security

trust

secure transactions

secure blocks

decentralized

recording information

technology involving

transactions

banking

cryptocurrency

almost impossible to hack

decentralized ledger

distributed technology

asymmetric cryptography

18

What is Blockchain?

- A Linked List
  - Replicated
  - Distributed
  - Consistency maintained by Consensus
  - Cryptographically linked
  - Cryptographically assured integrity of data
- Used as
  - Immutable Ledger of events, transactions or time stamped data
  - Tamper resistant log
  - Platform to Create and Transact in Cryptocurrency
  - log of events/transactions unrelated to currency

[Source – Lecture slides of Prof. Sandeep K. Shukla IIT Kanpur – NPTEL course]

Why a course on Blockchain?

- Have you seen the news lately?
  - Bitcoin
  - Ethereum
  - Blockchain for E-governance
  - Blockchain for supply chain management
  - Blockchain for energy management ……
  - Soon: Block chain for Nirvana
- Is it just a hype and hyperbole?
  - Hopefully this course will teach you otherwise
  - Even if you do not care about cryptocurrency and its market volatility

[Source – Lecture slides of Prof. Sandeep K. Shukla IIT Kanpur – NPTEL course]

Distributed Ledger Technology

- Distributed ledger technology (DLT) is a digital system for recording the transaction of assets in which the transaction and their details are recorded in multiple places at the same time.
- Unlike traditional databases, distributed ledgers have no control data store or administrative functionality.
- Blockchain is well known example of DLT.

[Source – Belotti, Marianna, et al. "A vademecum on blockchain technologies: When, which, and how." *IEEE Communications Surveys & Tutorials* 21.4 (2019): 3796-3838.]

Blockchain Technology

- Blockchain is an emerging technology and is a distributed ledger or a database that consists of non-erasable records of information.
- Blockchain is a distributed network and chain of cryptographic blocks combined together to form a Peer-to-Peer (P2P) network that is decentralized and distributed in nature.
- This technique allows users to share information among nodes in the network that do not trust each other

[Source –Aggarwal, Shubhani, et al. "Blockchain for smart communities: Applications, challenges and opportunities." *Journal of Network and Computer Applications* 144 (2019): 13-48.]

Blockchain Technology

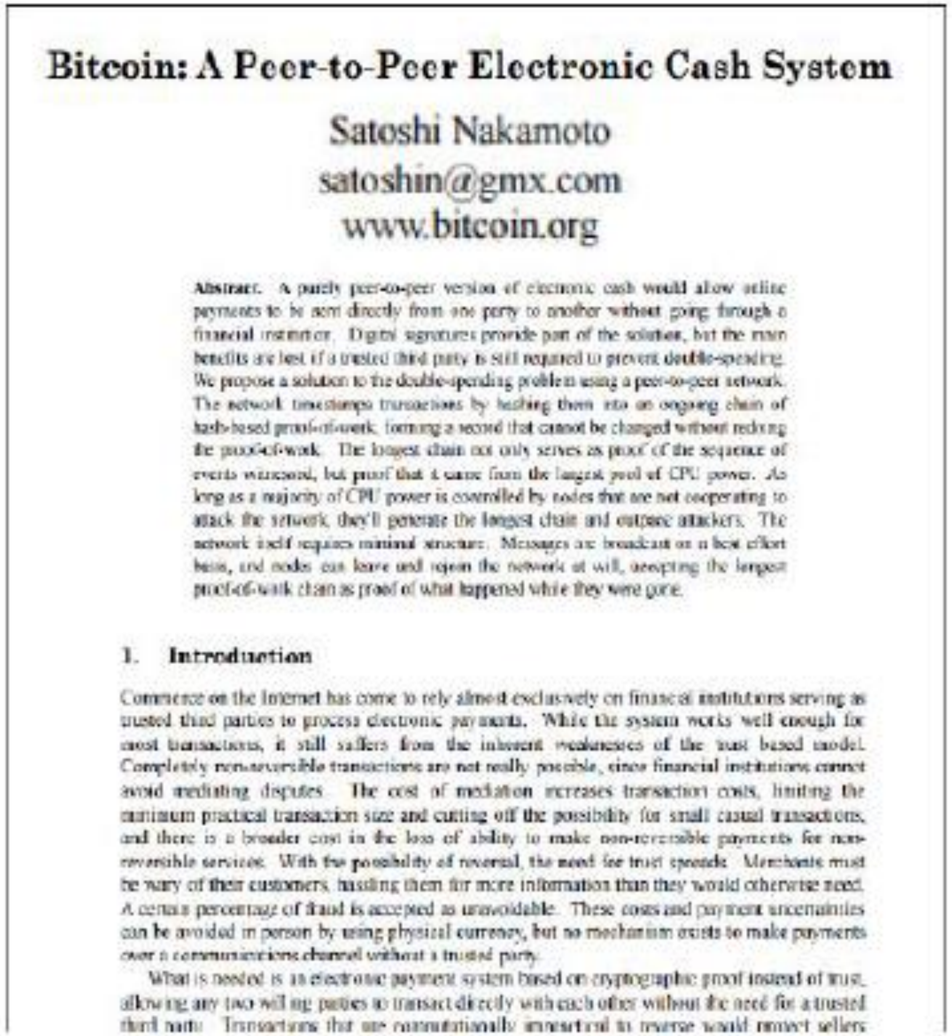
- The universally recognised father of blockchain technology is Satoshi Nakamoto that formally theorised and implemented it (2008 and 2009 respectively) as a core component of cryptocurrency Bitcoin.
- Types of cryptocurrencies are: Bitcoin, Bitcoin cash, Litcoin, Ethereum and many more

[Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Decentralized Business Review* (2008): 21260]

Bitcoin

2008: The Bitcoin white paper
2009: Reference implementation

Probably not this guy



Bitcoin: A Peer-to-Peer Electronic Cash System

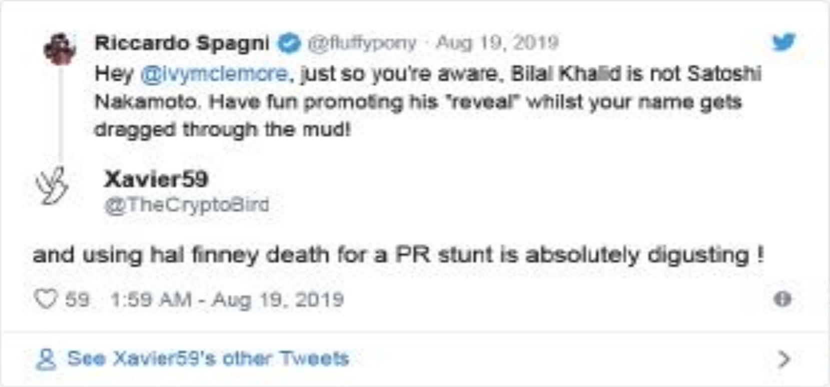
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers



Riccardo Spagni @fluffypony · Aug 19, 2019

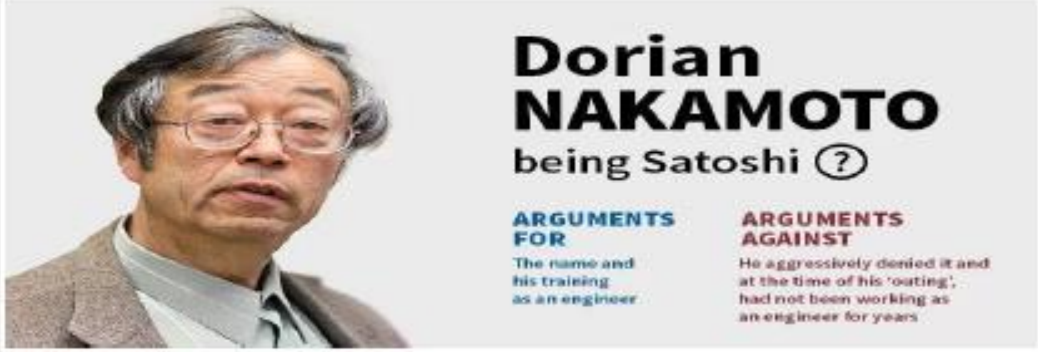
Hey @ivymclemore, just so you're aware, Bilal Khalid is not Satoshi Nakamoto. Have fun promoting his "reveal" whilst your name gets dragged through the mud!

Xavier59
@TheCryptoBird

and using hal finney death for a PR stunt is absolutely digusting !

♡ 59 1:59 AM - Aug 19, 2019

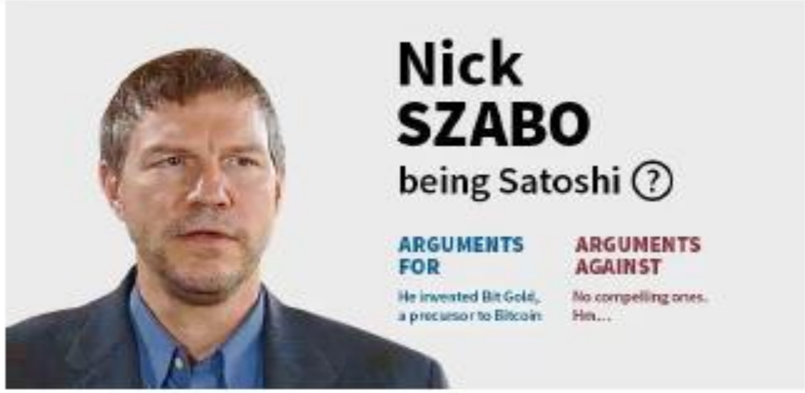
See Xavier59's other Tweets



Dorian NAKAMOTO being Satoshi ?

ARGUMENTS FOR
The name and his training as an engineer

ARGUMENTS AGAINST
He aggressively denied it and at the time of his 'outing', had not been working as an engineer for years



Nick SZABO being Satoshi ?

ARGUMENTS FOR
He invented Bit Gold, a precursor to Bitcoin

ARGUMENTS AGAINST
No compelling ones. Hm...

Craig WRIGHT being Satoshi ?

ARGUMENTS FOR
Timestamps of Nakomoto's blog coincide with Wright's blog

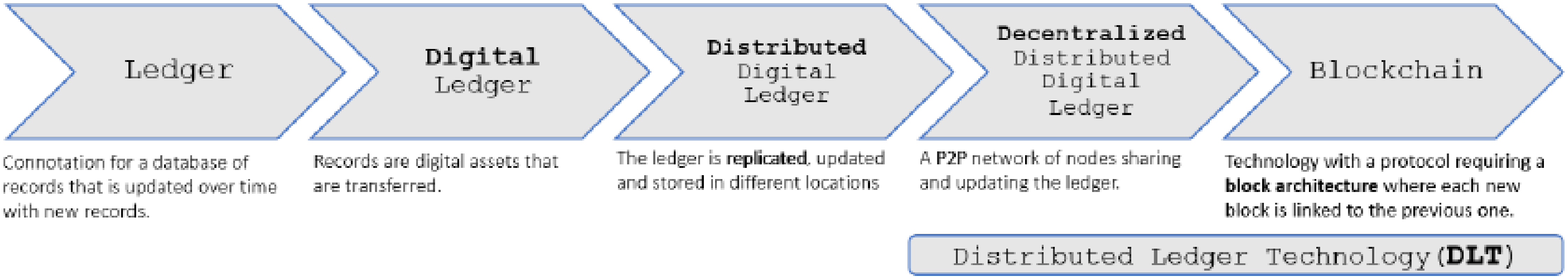
ARGUMENTS AGAINST
The PGP keys 'proving' he was founder were backdated, some allege

Source:

Satoshi Nakamoto:
The Mysterious Founder of Bitcoin

https://youtu.be/2Mlw_jVHq7U

DLT Evolution



Ledger

Connotation for a database of records that is updated over time with new records.

Digital Ledger

Records are digital assets that are transferred.

Distributed Digital Ledger

The ledger is **replicated**, updated and stored in different locations

Decentralized Distributed Digital Ledger

A **P2P** network of nodes sharing and updating the ledger.

Blockchain

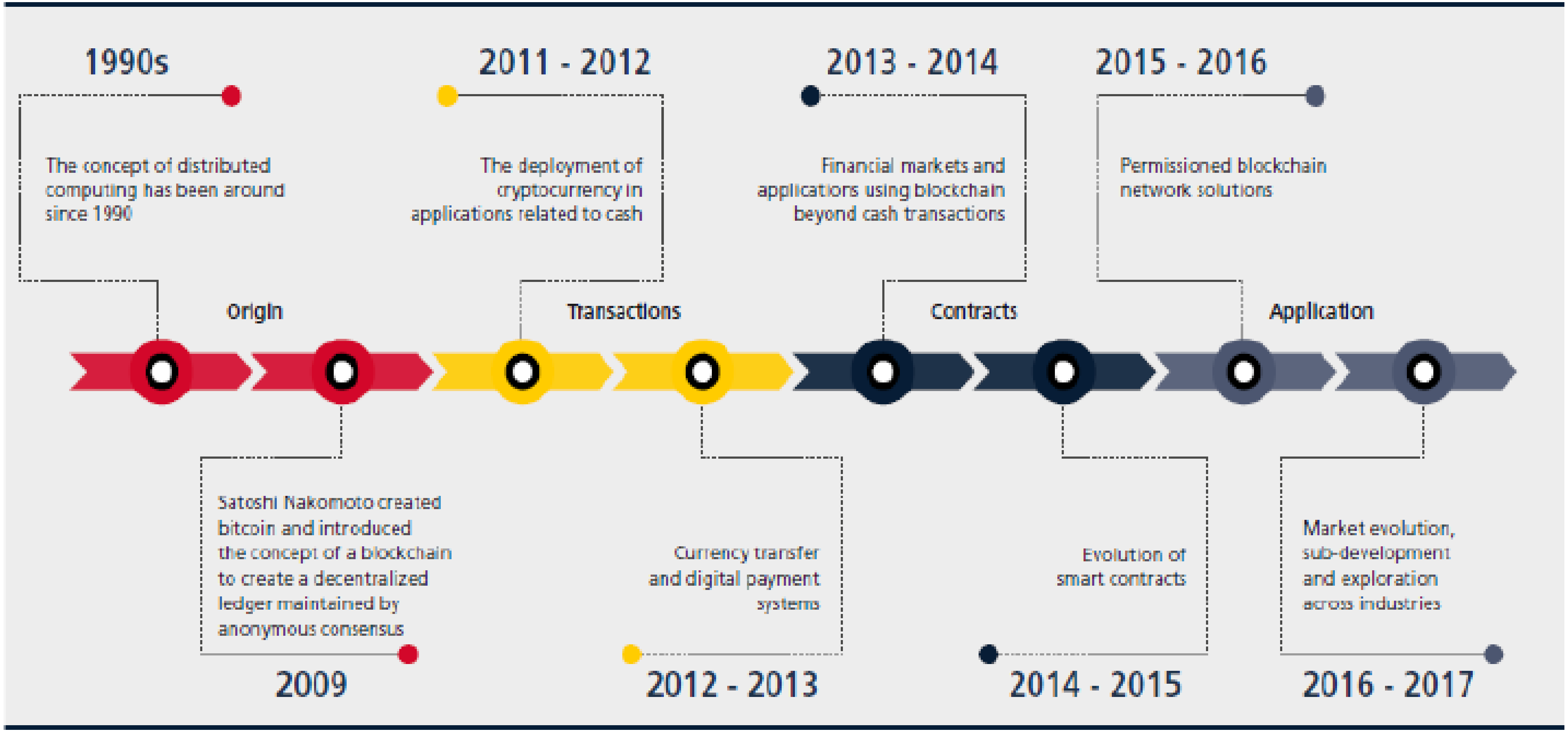
Technology with a protocol requiring a **block architecture** where each new block is linked to the previous one.

Distributed Ledger Technology (**DLT**)

DLT evolution: from the traditional ledger to blockchain.

[Source – Belotti, Marianna, et al. "A vademecum on blockchain technologies: When, which, and how." *IEEE Communications Surveys & Tutorials* 21.4 (2019): 3796-3838.]

BLOCKCHAIN HISTORY



1990s

The concept of distributed computing has been around since 1990

2009

Satoshi Nakomoto created bitcoin and introduced the concept of a blockchain to create a decentralized ledger maintained by anonymous consensus

2011 - 2012

The deployment of cryptocurrency in applications related to cash

2012 - 2013

Currency transfer and digital payment systems

2013 - 2014

Financial markets and applications using blockchain beyond cash transactions

2014 - 2015

Evolution of smart contracts

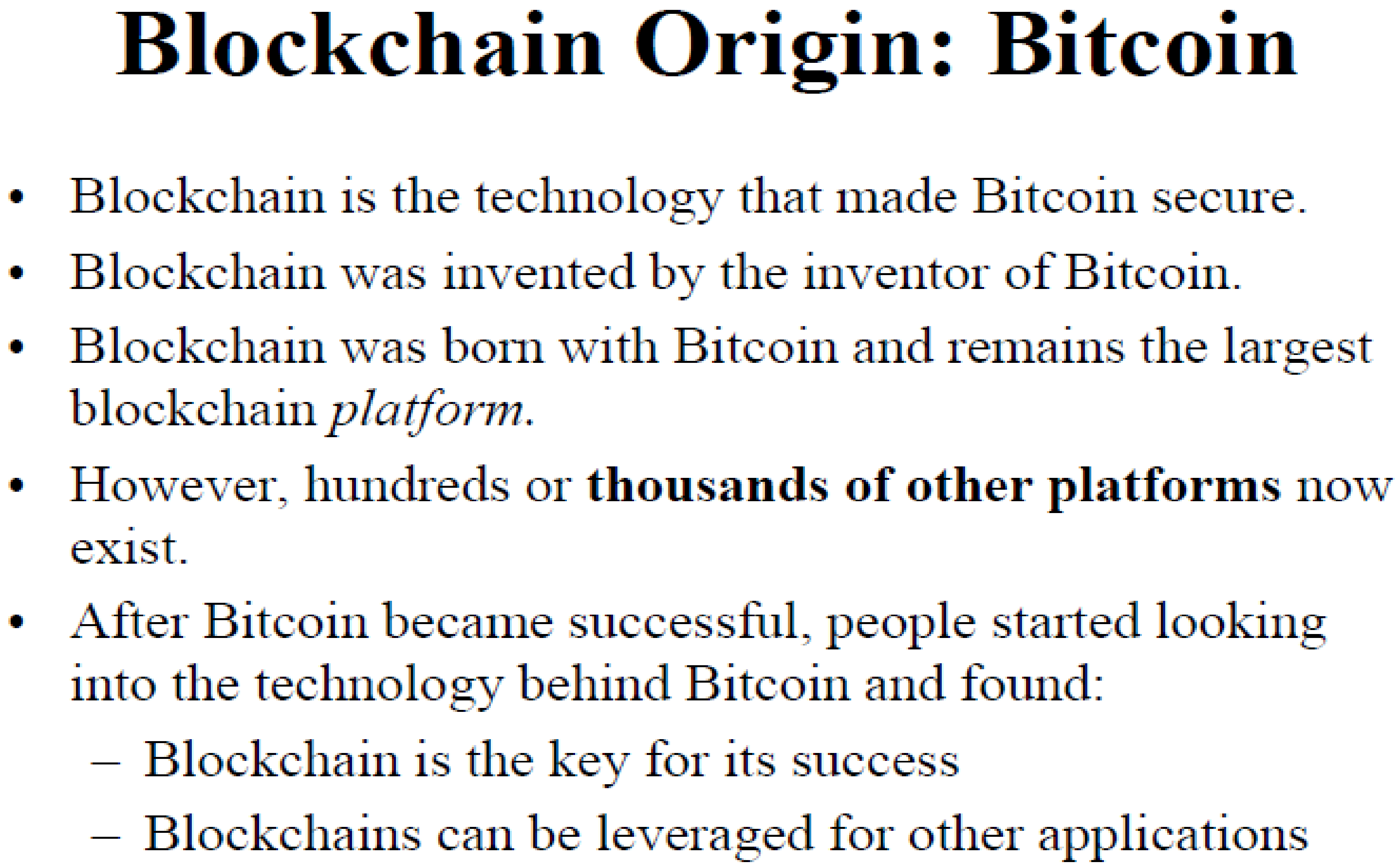
2015 - 2016

Permissioned blockchain network solutions

2016 - 2017

Market evolution, sub-development and exploration across industries

Figure 2: A history of blockchain technology; **Source:** Accenture



Blockchain Origin: Bitcoin

- Blockchain is the technology that made Bitcoin secure.
- Blockchain was invented by the inventor of Bitcoin.
- Blockchain was born with Bitcoin and remains the largest blockchain *platform*.
- However, hundreds or **thousands of other platforms** now exist.
- After Bitcoin became successful, people started looking into the technology behind Bitcoin and found:
  - Blockchain is the key for its success
  - Blockchains can be leveraged for other applications

[Source – Dr. Raju Halder, IIT Patna, Block ATAL FDP]

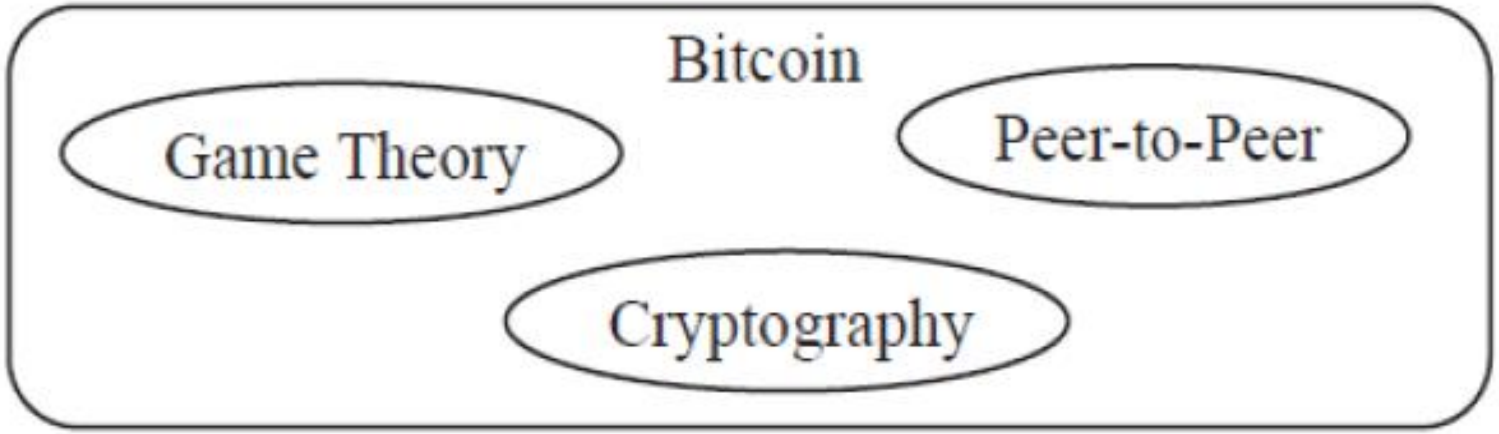
Blockchain Technolgy

Behind the success of Bitcoin

- IoT
- Supply Chain
- EHR
- Copyright Protection
- KYC
- Land Registry
- Data Sharing
- Cryptocurrency
- Smart Grid
- Insurance
- Smart Agriculture
- Smart Homes
- E-Commerce
- E-Governance
- Social Networking
- Education Certificate
- File Sharing
- Crowd Funding
- Postal System
- E-Voting
- Data Provenance
- E-Governance
- Asset Transfer
- Criminal Record Sharing
- Finance
- Many More....

[Source – Dr. Raju Halder, IIT Patna, Block ATAL FDP]

Bitcoin Technology



Bitcoin

Game Theory

Peer-to-Peer

Cryptography

- Bitcoin = Game Theory + Cryptography + P2P
- P2P: Information is stored throughout the global Internet
- Cryptography: Digital Signature, Message Authentication, Asymmetric Public/Private Key encryption, Hashing
- Game Theory: All activities are Win-Win.
  ⇒ People who store the chain, who mint the coin, all get paid.

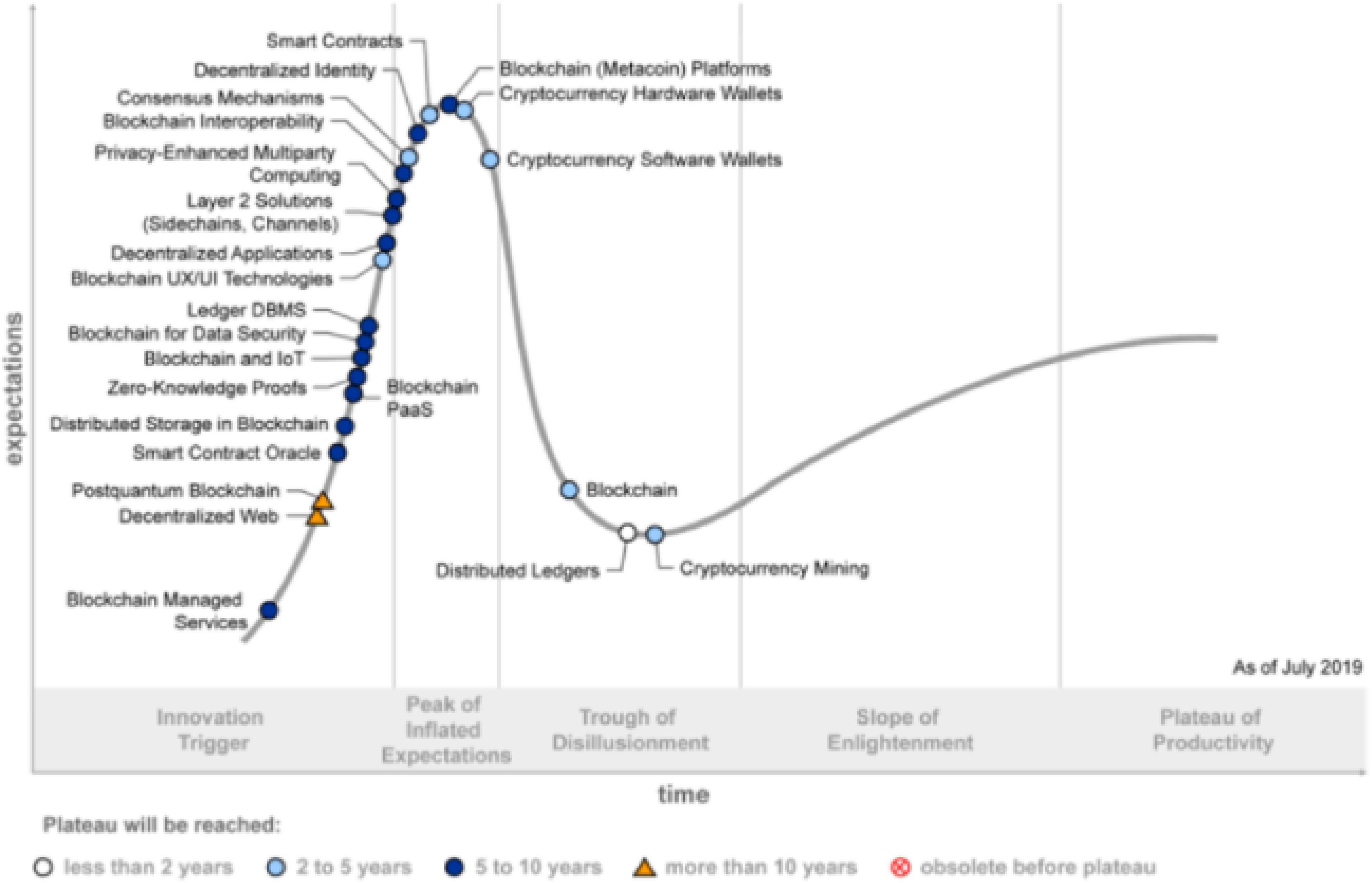
[Source – Dr. Raju Halder, IIT Patna, Block ATAL FDP]

Why Blockchain?

- Blockchain is a technology that increases transparency, as everybody on the network has a copy of the ledger.
- This makes the blockchain ledge tamper-proof.
- Blockchain is a safer way to record activity and keep data updated, while maintaining a record of its history.
- The features of the blockchain (*Decentralization, Immutability, auditability, Integrity, Authenticity, Non-Repudiation and fault tolernce)* make it attractive for various applications.

[Source – Belotti, Marianna, et al. "A vademecum on blockchain technologies: When, which, and how." *IEEE Communications Surveys & Tutorials* 21.4 (2019): 3796-3838.]

Figure 1: Hype Cycle for Blockchain Technologies, 2019



Source: Gartner (October 2019)

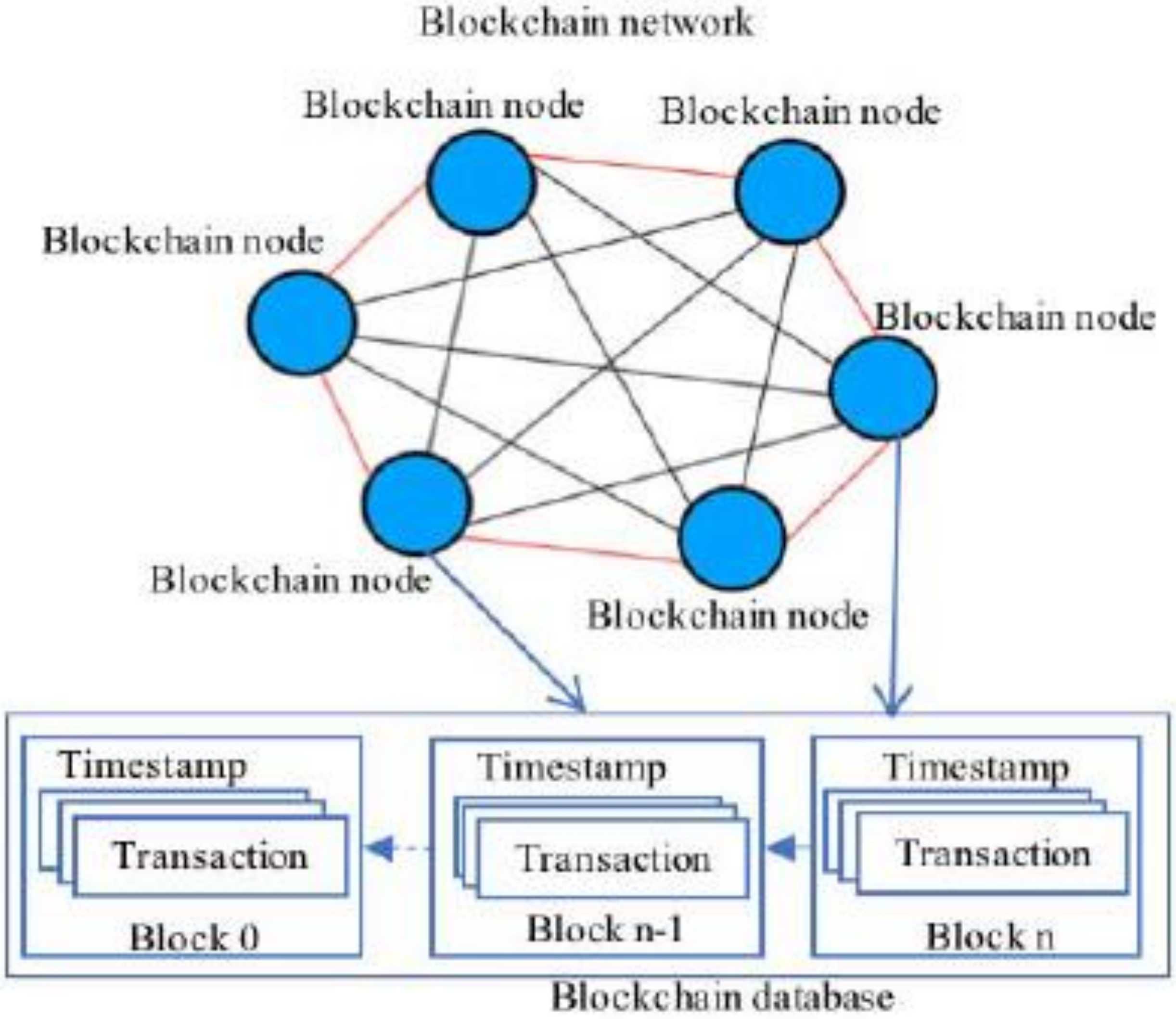


Fig. 2. Blockchain network, database, blocks, and transactions.

[Source : Salman, Tara, et al. "Security services using blockchains: A state of the art survey." *IEEE Communications Surveys & Tutorials* 21.1 (2018): 858-880.]

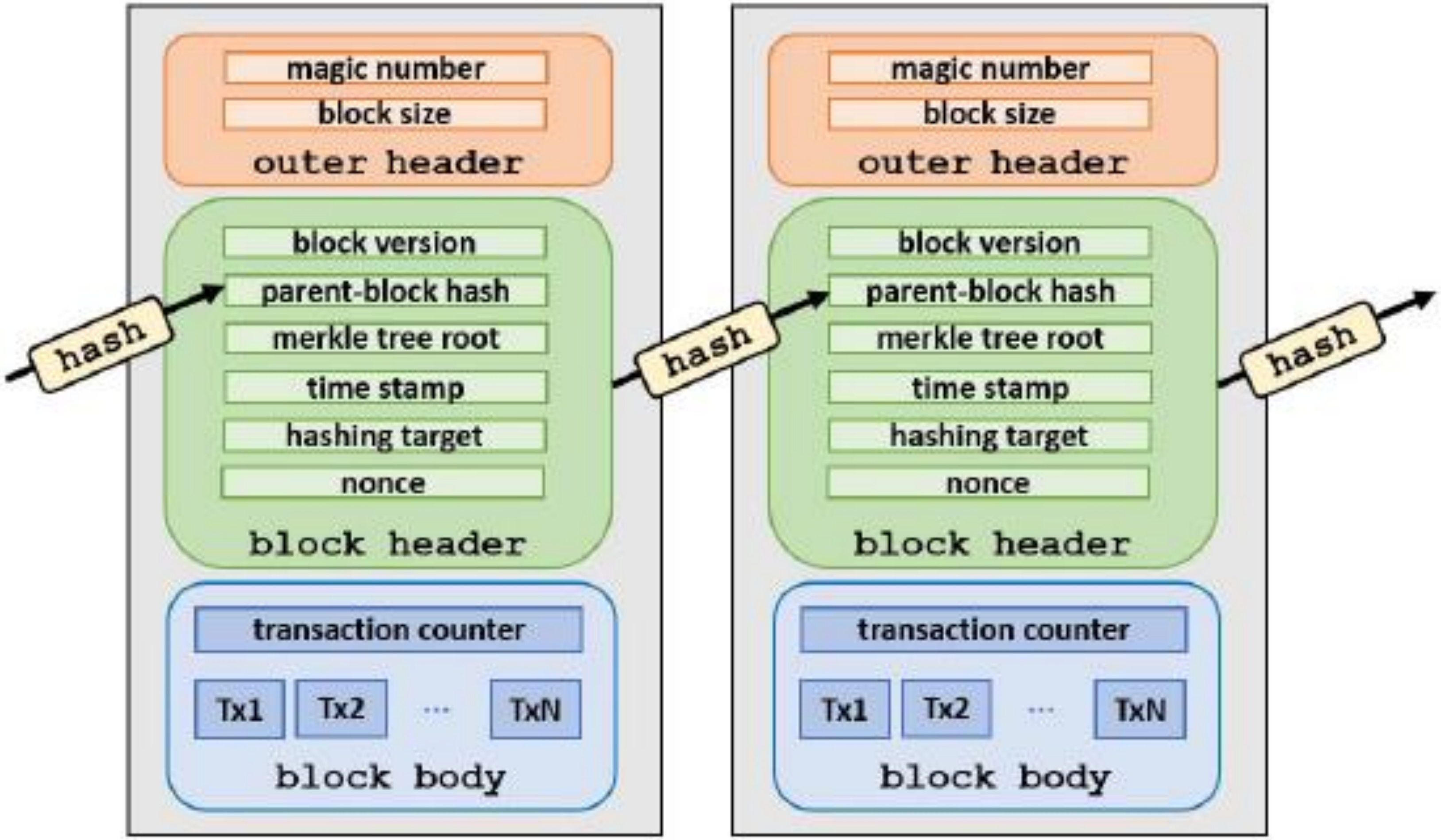


Fig. 6. Representation of a blockchain structure.

[Source – Belotti, Marianna, et al. "A vademecum on blockchain technologies: When, which, and how." *IEEE Communications Surveys & Tutorials* 21.4 (2019): 3796-3838.]

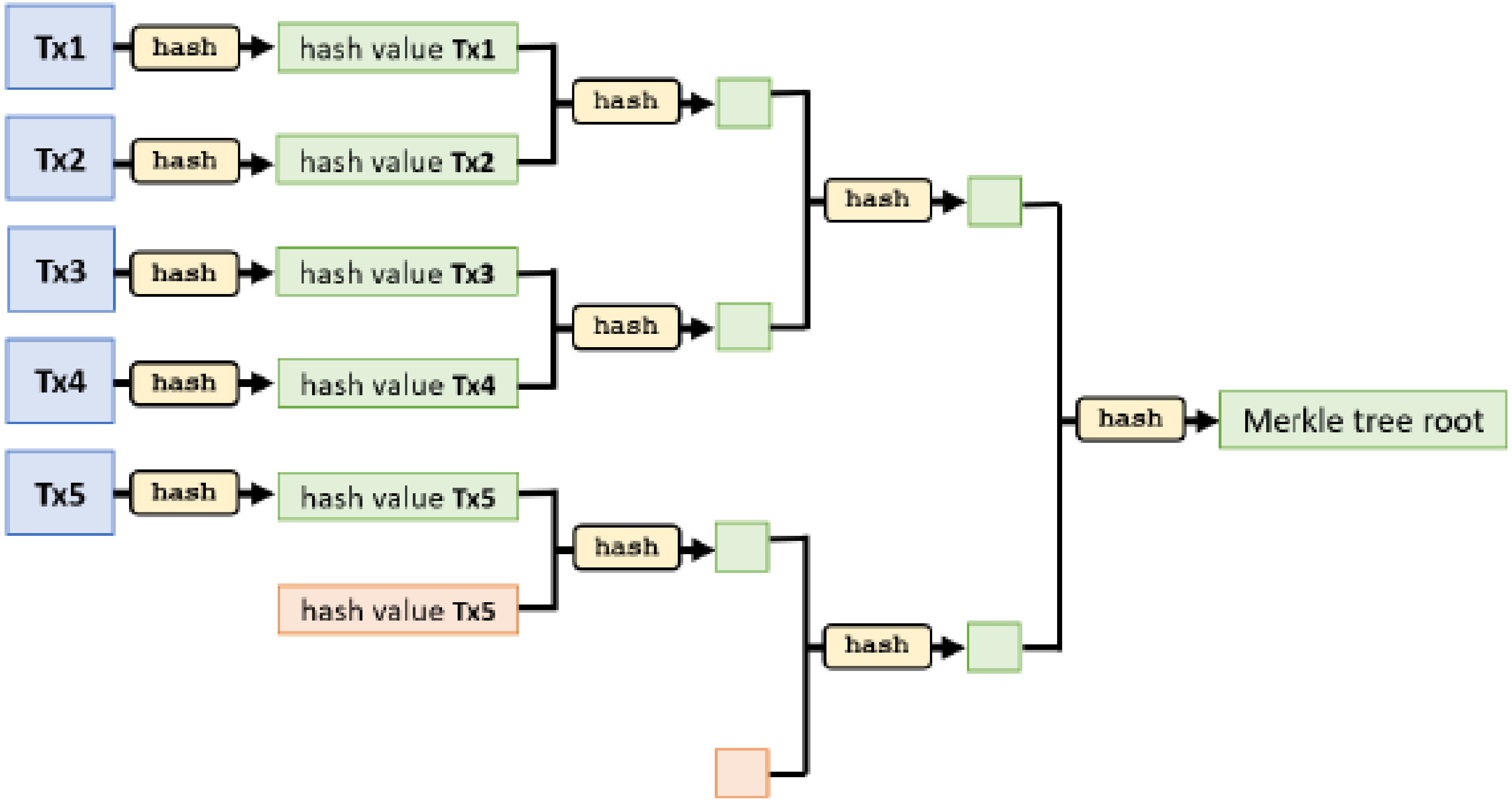
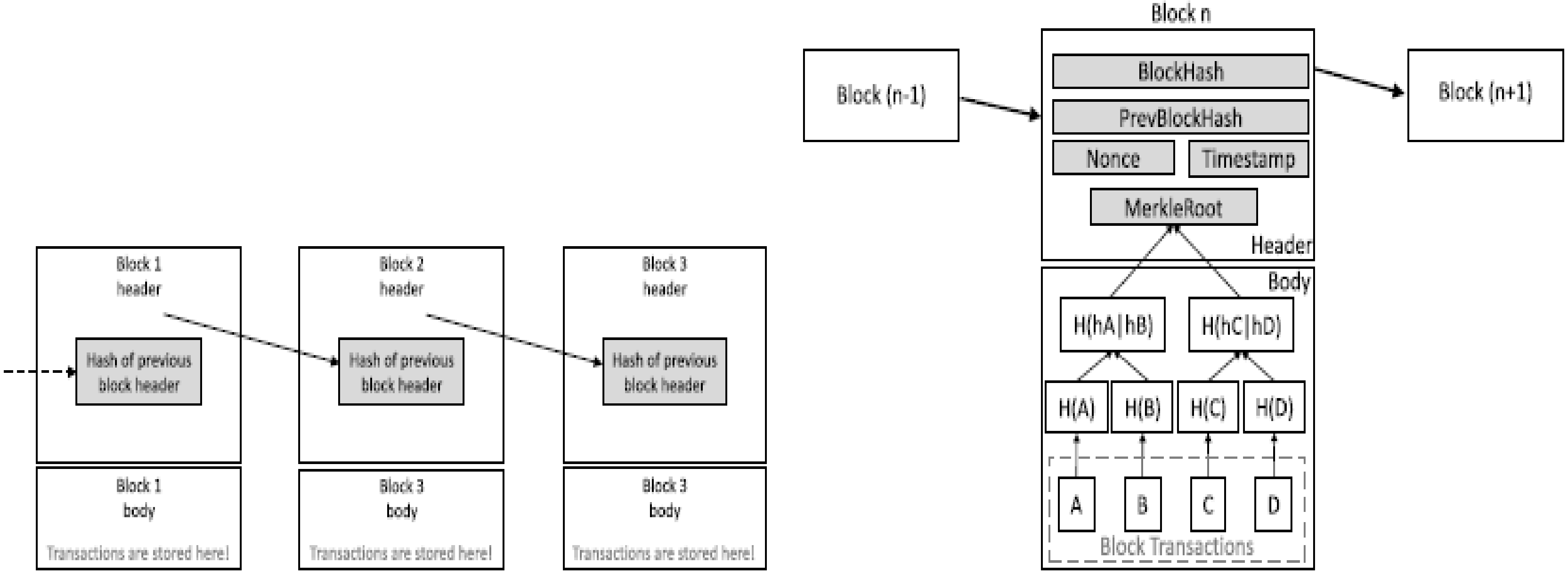


Fig. 7. Merkle hash tree procedure example: duplicated (hashed) transactions are marked in orange.

[Source – Belotti, Marianna, et al. "A vademecum on blockchain technologies: When, which, and how." *IEEE Communications Surveys & Tutorials* 21.4 (2019): 3796-3838.]



(a) Logical representation of a blockchain.

(b) Block header fields and Merkle tree for storing transactions in a block.

[Source: Ali, Muhammad Salek, et al. "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys & Tutorials 21.2 (2018): 1676-1717]

Important Terminology

- Transaction - A process that changes the state of the blockchain ledger. Depending on the application, the transaction can be the transfer of a financial value or the execution of a smart contract.
- Block – It consists of a block header and a block data.
- Block hash - It is the unique identifier of a particular block and is obtained by hashing the block header twice
- Merkle tree root hash: All the transactions in the block are hashed individually using a hashing algorithm. The hash values are then combined pairwise and are hashed again until a single hash value is obtained. This value is known as the merkle tree root hash value.
- Previous block hash - It is the hash of the block preceding the current block in the chain. The preceding block is known as the parent of the current block. The use of previous block's hash value in a block header is to ensure the immutability of blockchain ledger.
- Genesis block - This is the first block in the ledger. All the following blocks in the chain are linked to the genesis block. The genesis block generally includes the configuration for the network characteristics, the consensus protocol to be used, the access control rights, the hash function, the block generation interval, and the block size.
- Time stamp - It indicates the time at which the block is created.
- Block version - It indicates the version of the blockchain protocols used.
- Mining - It is the process of adding the valid transactions in a block and broadcasting that block to the network.
- Consensus protocols – Consensus protocols are used for validating transactions on the blockchain

[Source - Ismail, Leila, and Huned Materwala. "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions." *Symmetry* 11.10 (2019): 1198]

Terminology

- *A distributed ledger* is a type of digital data structure residing across multiple computer devices, generally at geographically distinguished locations
- *Distributed Ledger Technology (DLT)* designs a type of technology enabling storing and updating a distributed ledger in a decentralized manner.
- *A blockchain* is a P2P DLT structured as a chain of blocks, forged by consensus, which can be combined with a data model and a communication language enabling smart contracts and other assisting technologies.

[Source - Ismail, Leila, and Huned Materwala. "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions." *Symmetry* 11.10 (2019): 1198.

Terminology

- In all DLTs, there is an initial record - in a blockchain it is called a *genesis block*.
- The blockchain ledger consists of digital transactions representing interactions between nodes of a P2P network.
- *Transactions* are individual and indivisible operations that involve exchange or transfer of digital assets (information, goods, services, funds or set of rules which can trigger another transaction).

[Source - Ismail, Leila, and Huned Materwala. "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions." *Symmetry* 11.10 (2019): 1198.

Terminology

- *Blockchain nodes* are computing device connected to the blockchain that support the network by maintaining a copy of the ledger.
- Blockchain transactions are grouped into blocks, and there can be any number of transactions per block while respecting a given block size limit.
- Nodes on a blockchain network group up these transactions and send them throughout the network. Eventually peers synchronize to an exact copy of the blockchain throughout the network.

[Source - Ismail, Leila, and Huned Materwala. "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions." *Symmetry* 11.10 (2019): 1198.

Terminology

- The blockchain updating procedure needs a consensus, i.e., an agreement among the network peers.
- *Consensus* in the network refers to the process of achieving agreement among the network participants as to the correct state of data on the system.
- Consensus leads to all nodes sharing the exact same data.
- Therefore a consensus algorithm
  - – (*i*) ensures that the data on the ledger is the same for all network nodes, and
  - – (*ii*) prevents malicious actors from manipulating the data.

[Source - Ismail, Leila, and Huned Materwala. "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions." *Symmetry* 11.10 (2019): 1198.

Terminology

- The consensus procedure varies with different blockchain implementations.
- The Bitcoin blockchain uses a *PoW* based consensus mechanism, other blockchains and distributed ledgers are deploying a variety of consensus algorithms belonging to two main classes:
  - (*i*) *Proof-of-X*-based algorithms and
  - (*ii*) *Byzantine Fault Tolerant* algorithms.

[Source - Ismail, Leila, and Huned Materwala. "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions." *Symmetry* 11.10 (2019): 1198.

Terminology

- A generic DLT can fit any digital asset exchange requirement. Contractual aspects of an exchange, involving nodes’ rights and obligations, can be digitalized and controlled by proper digital (smart) contracts.
- A *smart contract* is a computer program that executes predefined actions when certain conditions within the system are met.
- Smart contracts provide the transactions language allowing the ledger state to be modified.
- They can facilitate the exchange and transfer of any asset (e.g., shares, currency, content, property).

[Source - Ismail, Leila, and Huned Materwala. "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions." *Symmetry* 11.10 (2019): 1198.

Terminology

- *Blockchain* – the actual ledger
- *Blockchain technology* – a term to describe the technology in the most generic form
- *Blockchain network* – the network in which a blockchain is being used
- *Blockchain implementation* – a specific blockchain
- *Blockchain network user* – a person, organization, entity, business, government, etc. which is utilizing the blockchain network

- *Node* – an individual system within a blockchain network
  - *Full node* – a node that stores the entire blockchain, ensures transactions are valid
    - *Publishing node* – a full node that also publishes new blocks
  - *Lightweight node* – a node that does not store or maintain a copy of the blockchain and must pass their transactions to full nodes

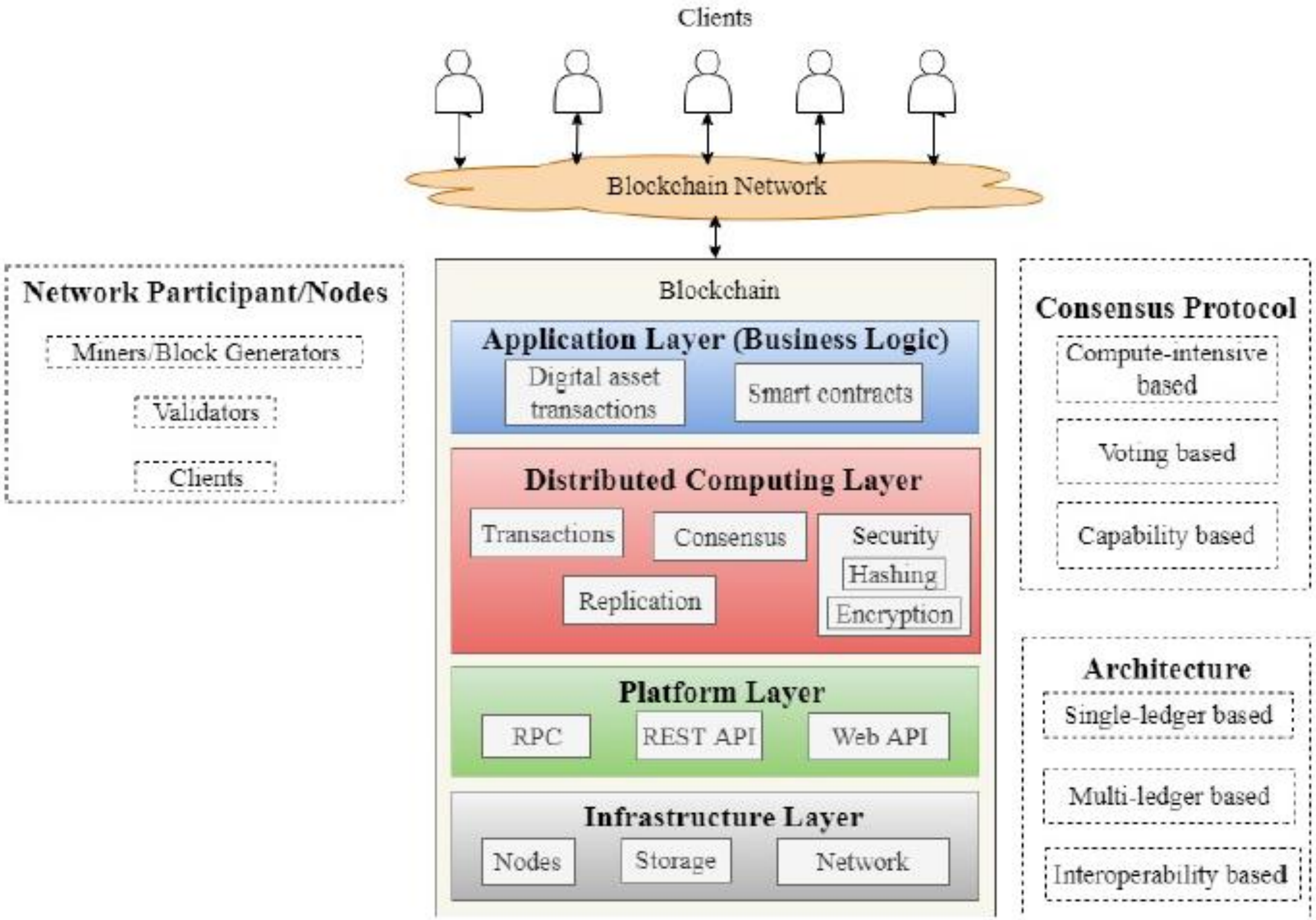


Figure 1. Overview of Blockchain.

3.1. Blockchain Overview

[Source - Ismail, Leila, and Huned Materwala. "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions." *Symmetry* 11.10 (2019): 1198.

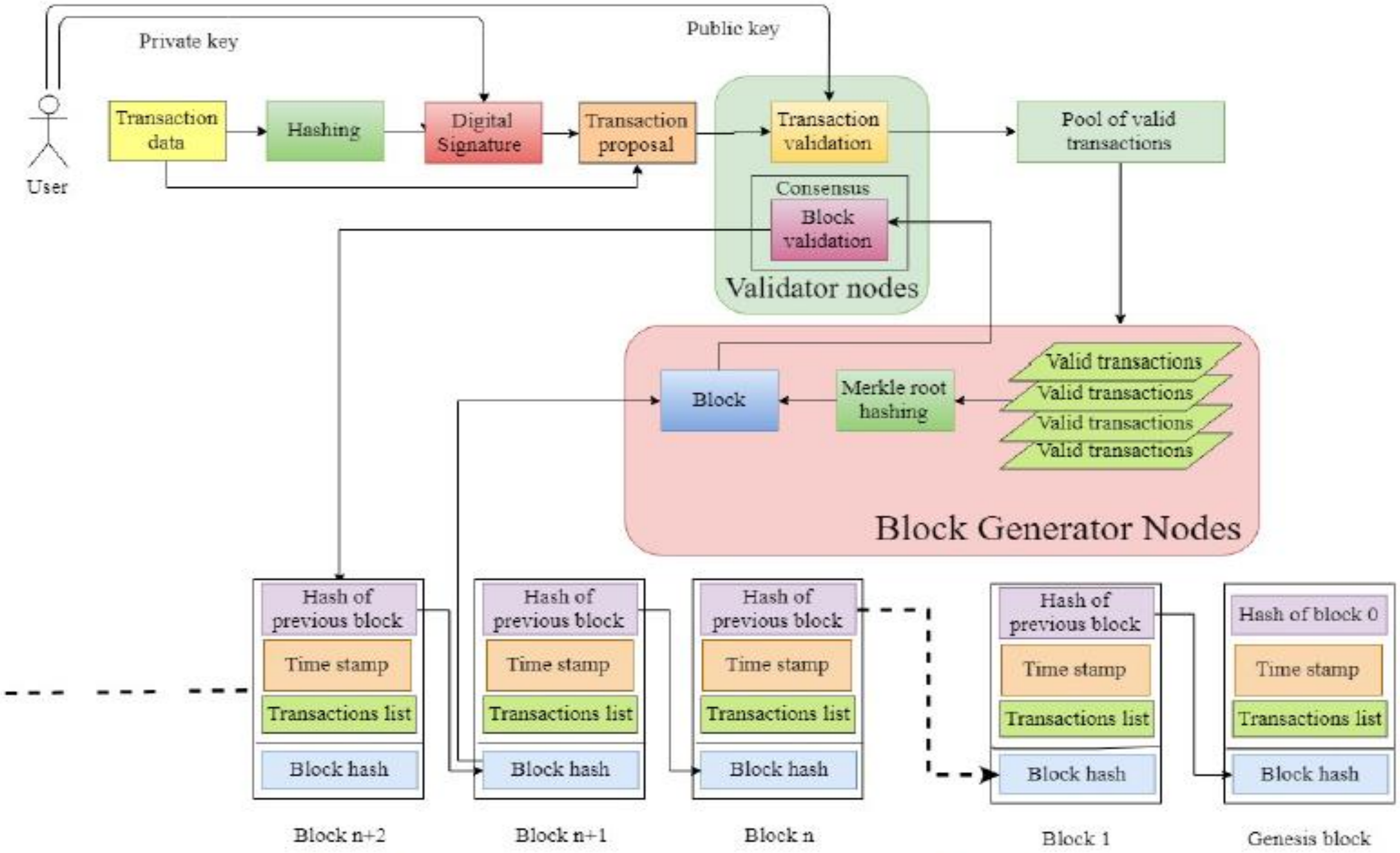


Figure 2. Overview of Transaction Execution Flow in Blockchain.

[Source - Ismail, Leila, and Huned Materwala. "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions." *Symmetry* 11.10 (2019): 1198]

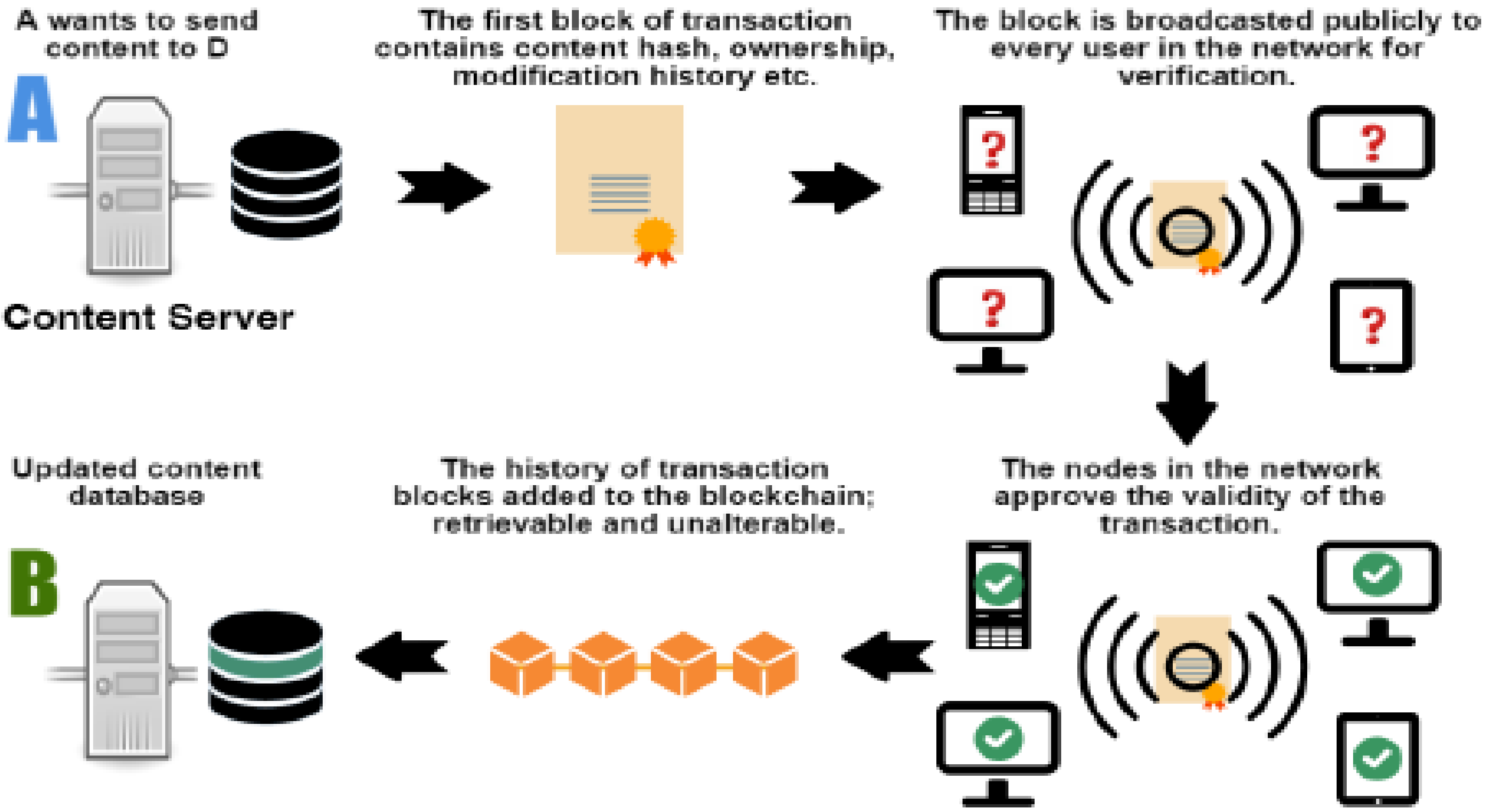
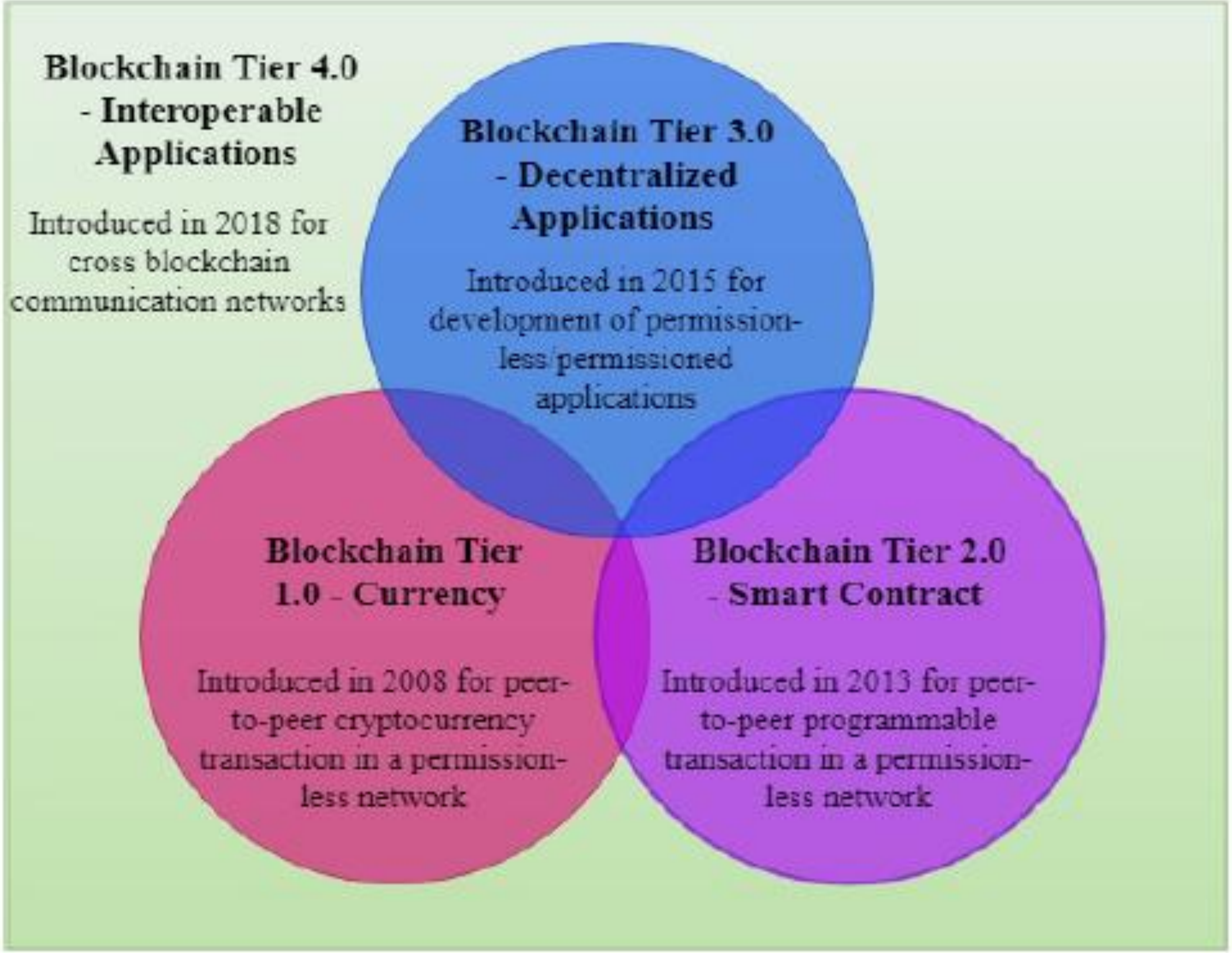

A wants to send content to D
A
Content Server
The first block of transaction contains content hash, ownership, modification history etc.
The block is broadcasted publicly to every user in the network for verification.
?
The nodes in the network approve the validity of the transaction.
The history of transaction blocks added to the blockchain; retrievable and unalterable.
Updated content database
B

Fig. 1. Overview of the blockchain working principle.

[Source: Bhowmik, Deepayan, and Tian Feng. "The multimedia blockchain: A distributed and tamper-proof media transaction framework." *2017 22nd International Conference on Digital Signal Processing (DSP)*. IEEE, 2017.]



Blockchain Tier 4.0 - Interoperable Applications

Introduced in 2018 for cross blockchain communication networks

Blockchain Tier 3.0 - Decentralized Applications

Introduced in 2015 for development of permission-less/permissioned applications

Blockchain Tier 1.0 - Currency

Introduced in 2008 for peer-to-peer cryptocurrency transaction in a permission-less network

Blockchain Tier 2.0 - Smart Contract

Introduced in 2013 for peer-to-peer programmable transaction in a permission-less network

Figure 5. Blockchain Tiers.

[Source - Ismail, Leila, and Huned Materwala. "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions." *Symmetry* 11.10 (2019): 1198]

Salient features of the blockchain

- *Decentralization:* In blockchain-based infrastructures, two nodes can engage in transactions with each other without the need to place trust upon a central entity to maintain records or perform authorization.

- *Immutability:* Since all new entries made in the blockchain are agreed upon by peers via decentralized consensus, the blockchain is censorship-resistant and is nearly impossible to tamper. Similarly, all previously held records in the blockchain are also immutable and, in order to alter any previous records, an attacker would need to compromise a majority of the nodes involved in the blockchain network. Otherwise, any changes in the blockchain contents are easily detected.

- *Auditability :* All peers hold a copy of the blockchain, and can thus access all timestamped transaction records. This transparency allows peers to look up and verify transactions involving specific blockchain addresses. Blockchain addresses are not associated with identities in real life, so the blockchain provides a manner of pseudo-anonymity.

[Source: Ali, Muhammad Salek, et al. "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys & Tutorials 21.2 (2018): 1676-1717]

Salient features of the blockchain

- *Integrity, Authenticity, Non-Repudiation :* The data hashing grants that data is not modified during its transmission (i.e., integrity). Moreover, the origin of a transaction can be ascertained by the senders' public key dissemination, while the evidence of the sending action is represented by the data signing procedure involving the private key (i.e., authenticity and non-repudiation).

- *fault tolerance:* All blockchain peers contain identical replicas of the ledger records. Any faults or data leakages that occur in the blockchain network can be identified through decentralized consensus, and data leakages can be mitigated using the replicas stored in blockchain peers.

[Source: Ali, Muhammad Salek, et al. "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys & Tutorials 21.2 (2018): 1676-1717]

Types of blockchain

- *Public Blockchains*
- *Private Blockchains*
- *Consortium Blockchains*

Ali, Muhammad Salek, et al. "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys & Tutorials 21.2 (2018): 1676-1717.

Types of blockchain

- *Public Blockchains:* Public blockchains are truly decentralized, where all members can participate in publishing new blocks and accessing blockchain contents.
- Public blockchains are termed *permissionless* in that it allows anyone to maintain a copy of the blockchain and engage in validating new blocks. Examples of public blockchain implementation are cryptocurrency networks, such as Bitcoin, Ethereum, and so on.
- Publishing new blocks in a public blockchain involves either computationally expensive puzzle solving, or staking one’s own cryptocurrency. Each transaction has a processing fee attached to it, which serves as an incentive to the peers attempting to publish new blocks onto the blockchain.

Ali, Muhammad Salek, et al. "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys & Tutorials 21.2 (2018): 1676-1717.

Types of blockchain

- *Private Blockchains:* private blockchains are *permissioned*, and every node joining the network is a known member of a single organization.
- Private blockchains are suited for single enterprise solutions and are utilized as a synchronized distributed database meant to keep track of data exchanges occurring between different departments or individuals.

Ali, Muhammad Salek, et al. "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys & Tutorials 21.2 (2018): 1676-1717.

Types of blockchain

- *Private Blockchains:* private blockchains are *permissioned*, and every node joining the network is a known member of a single organization.
- Private blockchains are suited for single enterprise solutions and are utilized as a synchronized distributed database meant to keep track of data exchanges occurring between different departments or individuals.
- Private blockchains do not require currency or tokens to function, and there are no processing fees included in its transactions.
- Since blocks are published by delegated nodes within the network, a private blockchain is not as tamper-resistant as a public blockchain, and the organization may choose to roll back their blockchain to any point in the past.

Ali, Muhammad Salek, et al. "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys & Tutorials 21.2 (2018): 1676-1717.

Types of blockchain

- *Consortium Blockchains:* Consortium blockchains, or federated blockchains, are similar to private blockchains in the sense that it is a permissioned network.
- Consortium networks span multiple organizations and help maintain transparency among the involved parties.
- A consortium blockchain is used as an auditable and reliably synchronized distributed database, that keeps track of data exchanges taking place between the participating consortium members.
- While it does provide auditability and lower latency in transaction processing, it is not entirely decentralized or censorship-resistant.

Ali, Muhammad Salek, et al. "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys & Tutorials 21.2 (2018): 1676-1717.

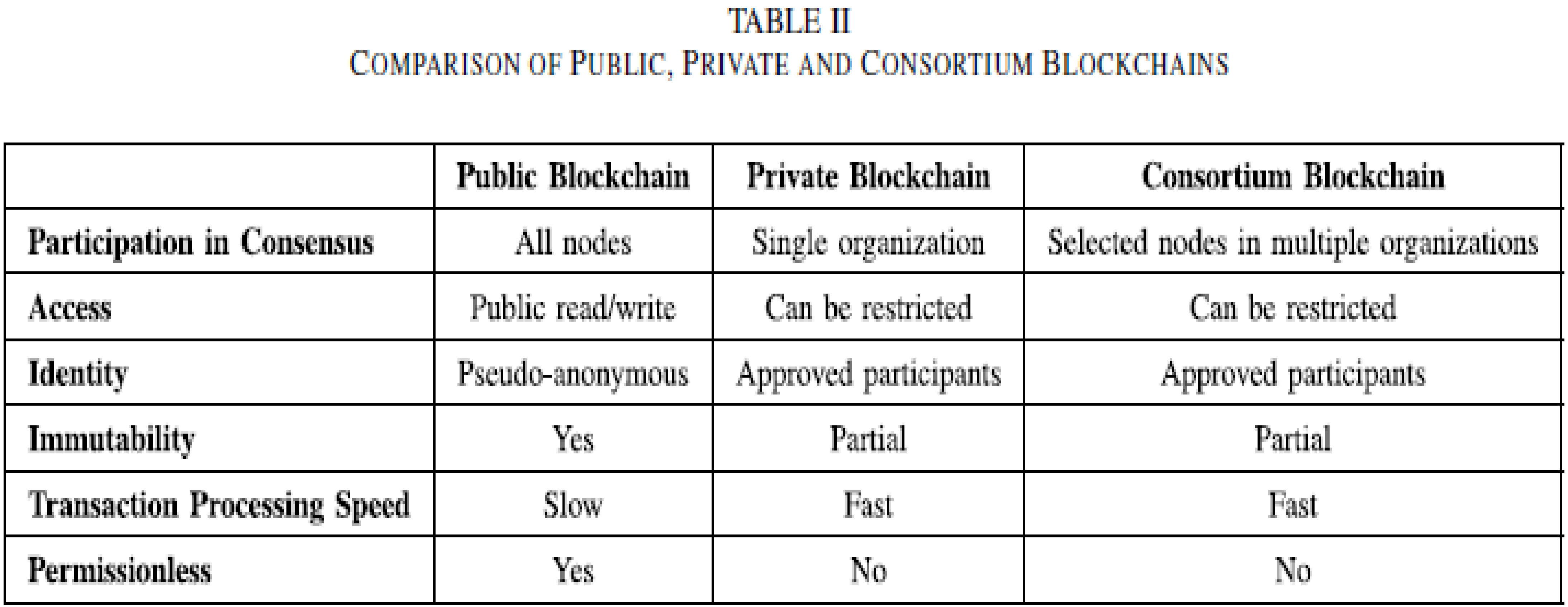


TABLE II
COMPARISON OF PUBLIC, PRIVATE AND CONSORTIUM BLOCKCHAINS

	Public Blockchain	Private Blockchain	Consortium Blockchain
Participation in Consensus	All nodes	Single organization	Selected nodes in multiple organizations
Access	Public read/write	Can be restricted	Can be restricted
Identity	Pseudo-anonymous	Approved participants	Approved participants
Immutability	Yes	Partial	Partial
Transaction Processing Speed	Slow	Fast	Fast
Permissionless	Yes	No	No

Ali, Muhammad Salek, et al. "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys & Tutorials 21.2 (2018): 1676-1717.

Blockchain Components

- **Cryptographic Hash Functions :** Within a blockchain network, cryptographic hash functions are used for many tasks, such as:
  - Address derivation : public key →cryptographic hash function → address
  - Creating unique identifiers.
  - Securing the block data – a publishing node will hash the block data, creating a digest that will be stored within the block header.
  - Securing the block header – a publishing node will hash the block header.
  - If the blockchain network utilizes a proof of work consensus model, the publishing node will need to hash the block header with different nonce values until the puzzle requirements have been fulfilled.
  - The current block header’s hash digest will be included within the next block’s header, where it will secure the current block header data.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Cryptographic Nonce :

- A cryptographic nonce is an arbitrary number that is only used once.
- A cryptographic nonce can be combined with data to produce different hash digests per nonce:

  hash (data + nonce) = digest
- Only changing the nonce value provides a mechanism for obtaining different digest values while keeping the same data.
- This technique is utilized in the proof of work consensus model

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Transactions :

- A *transaction* represents an interaction between parties.

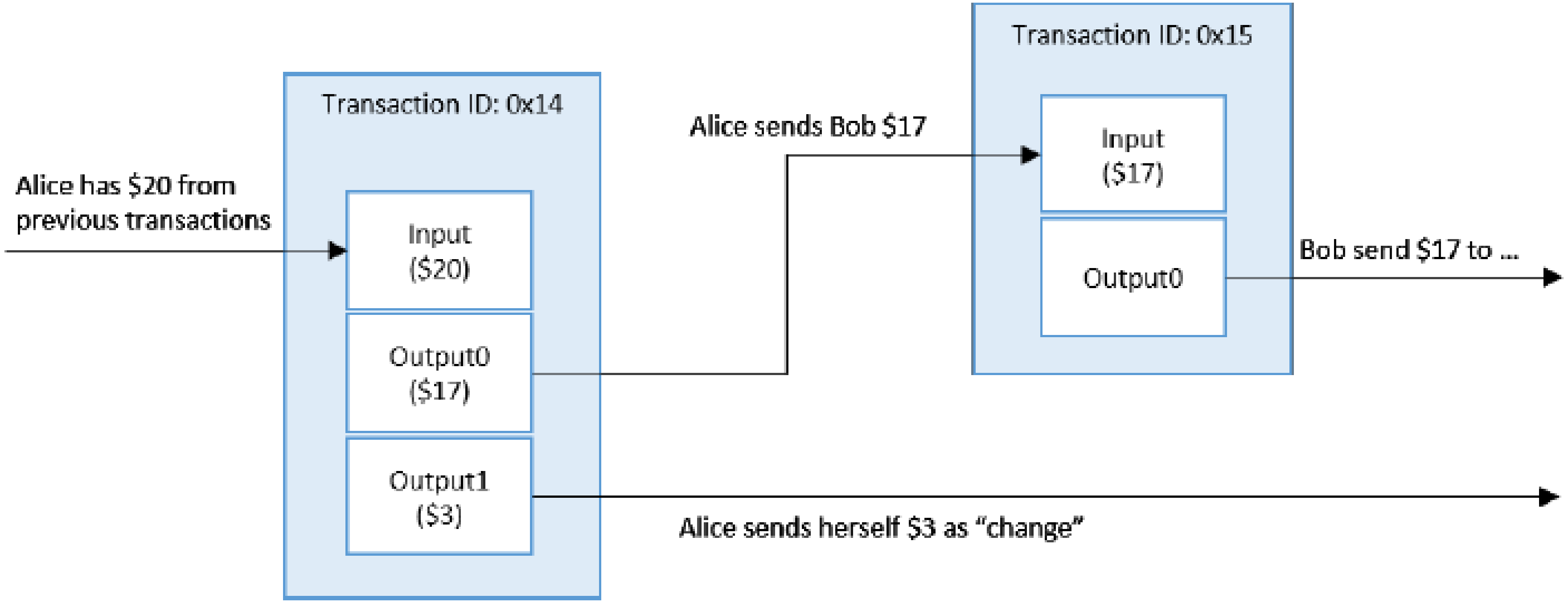


Figure 1 - Example Cryptocurrency Transaction

Blockchain Components

Asymmetric-Key Cryptography :

- A summary of the use of asymmetric-key cryptography in many blockchain networks:
  - Private keys are used to digitally sign transactions.
  - Public keys are used to derive addresses.
  - Public keys are used to verify signatures generated with private keys.
  - Asymmetric-key cryptography provides the ability to verify that the user transferring value to another user is in possession of the private key capable of signing the transaction.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Addresses and Address Derivation :

- Most blockchain implementations make use of addresses as the “to” and “from” endpoints in a transaction.
- Addresses are shorter than the public keys and are not secret.
- One method to generate an address is to create a public key, applying a cryptographic hash function to it, and converting the hash to text:

public key → cryptographic hash function → address

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Private Key Storage :

- With some blockchain networks (especially with permissionless blockchain networks), users must manage and securely store their own private keys.
- Instead of recording them manually, they often use software to securely store them. This software is often referred to as a *wallet*.
- The wallet can store private keys, public keys, and associated addresses. It may also perform other functions, such as calculating the total number of digital assets a user may have.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Private Key Storage :

- If a user loses a private key, then any digital asset associated with that key is lost, because it is computationally infeasible to regenerate the same private key.
- If a private key is stolen, the attacker will have full access to all digital assets controlled by that private key.
- The security of private keys is so important that many users use special secure hardware to store them; alternatively, users may take advantage of an emerging industry of private key escrow services.
- These key escrow services can also satisfy KYC laws in addition to storing private keys as users must provide proof of their identity when creating an account.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Ledgers :

- A *ledger* is a collection of transactions.
- Throughout history, pen and paper ledgers have been used to keep track of the exchange of goods and services.
- In modern times, ledgers have been stored digitally, often in large databases owned and operated by a centralized trusted third party (i.e., the owner of the ledger) on behalf of a community of users.
- These ledgers with centralized ownership can be implemented in a centralized or distributed fashion (i.e., just one server or a coordinating cluster of servers).

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Ledgers :

- Blockchain technology enables such an approach using both distributed ownership as well as a distributed physical architecture.
- The distributed physical architecture of blockchain networks often involve a much larger set of computers than is typical for centrally managed distributed physical architecture.
- The growing interest in distributed ownership of ledgers is due to possible trust, security, and reliability concerns related to ledgers with centralized ownership:

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Blocks :

- Blockchain network users submit candidate transactions to the blockchain network via software (desktop applications, smartphone applications, digital wallets, web services, etc.)
- The software sends these transactions to a node or nodes within the blockchain network.
- For many blockchain implementations, once a pending transaction has been distributed to nodes, it must then wait in a queue until it is added to the blockchain by a publishing node.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Blocks :

- The block data contains a list of validated and authentic transactions which have been submitted to the blockchain network.
- Validity and authenticity is ensured by checking that the transaction is correctly formatted and that the providers of digital assets in each transaction (listed in the transaction's 'input' values) have each cryptographically signed the transaction.
- This verifies that the providers of digital assets for a transaction had access to the private key which could sign over the available digital assets.
- The other full nodes will check the validity and authenticity of all transactions in a published block and will not accept a block if it contains invalid transactions.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Blocks :

- Block Header
  - – The block number, also known as block height in some blockchain networks.
  - – The previous block header’s hash value.
  - – A hash representation of the block data (different methods can be used to accomplish this, such as a generating a Merkle tree (defined in Appendix B), and storing the root hash, or by utilizing a hash of all the combined block data).
  - – A timestamp.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Blocks :

- Block Header
  - The size of the block.
  - The nonce value. For blockchain networks which utilize mining, this is a number which is manipulated by the publishing node to solve the hash puzzle.
  - Other blockchain networks may or may not include it or use it for another purpose other than solving a hash puzzle.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Blockchain Components

Blocks :

- Block Data
  - – A list of transactions and ledger events included within the block.
  - – Other data may be present.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Pseudonymous

- In Bitcoin, the blockchain enabled users to be pseudonymous.
- This means that users are anonymous, but their account identifiers are not; additionally, all transactions are publicly visible.
- This has effectively enabled Bitcoin to offer pseudo-anonymity because accounts can be created without any identification or authorization process (such processes are typically required by Know-Your-Customer (KYC) laws).

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Consensus Models

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Round Robin
- Proof of Authority/Proof of Identity
- Proof of Elapsed Time (PoET)
- ….

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Work (PoW)

- Proof of Work (PoW)
  - In the proof of work (PoW) model, a user publishes the next block by being the first to solve a computationally intensive puzzle.
  - The solution to this puzzle is the “proof” they have performed work.
  - The puzzle is designed such that solving the puzzle is difficult but checking that a solution is valid is easy.
  - This enables all other full nodes to easily validate any proposed next blocks, and any proposed block that did not satisfy the puzzle would be rejected.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Work (PoW)

- hash (data + nonce) = digest

- 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**”

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Work (PoW)

SHA256(“blockchain” + Nonce) = Hash Digest starting with “**000000**”

- SHA256("blockchain0") = 0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938 (not solved)
- SHA256("blockchain1") = 0xdb0b9c1cb5e9c680dfff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10 (not solved)
- …
- SHA256("blockchain10730895") = 0x**000000**ca1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587 (solved)

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Work (PoW)

- In this example, each additional “leading zero” value increases the difficulty.
- By increasing the target by one additional leading zero (“**0000000**”), the same hardware took 934,224,175 guesses to solve the puzzle (completed in 1 hour, 18 minutes, 12 seconds):

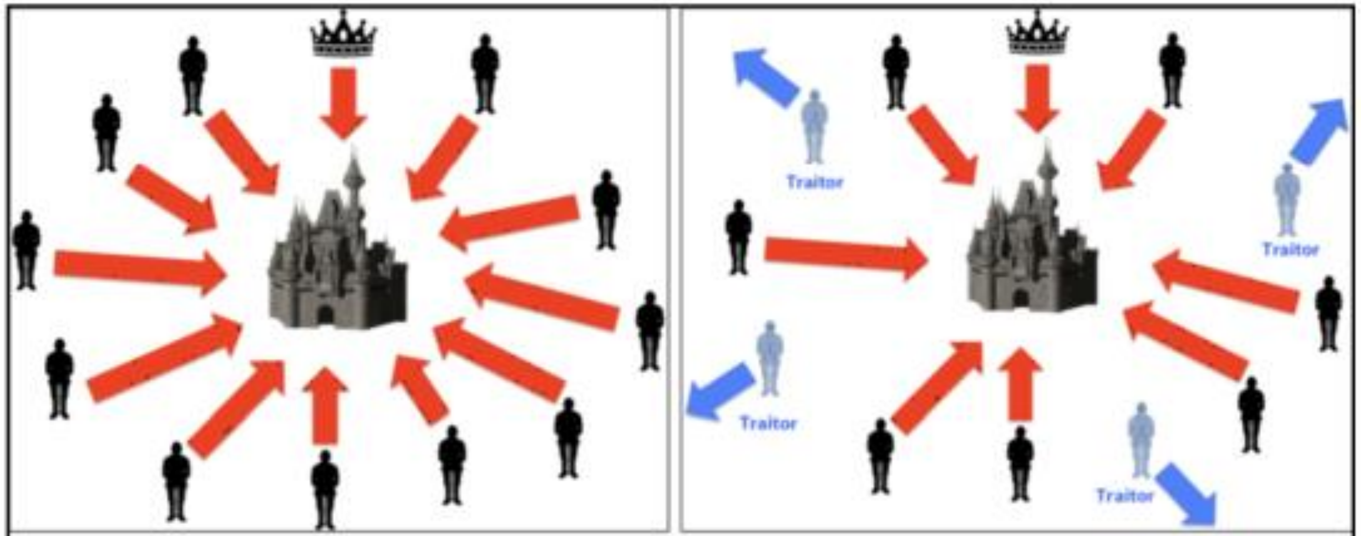
SHA256("blockchain934224174") =
0x**0000000**e2ae7e4240df80692b7e586ea7a977eacbd031819d0e603257edb3a81

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Work

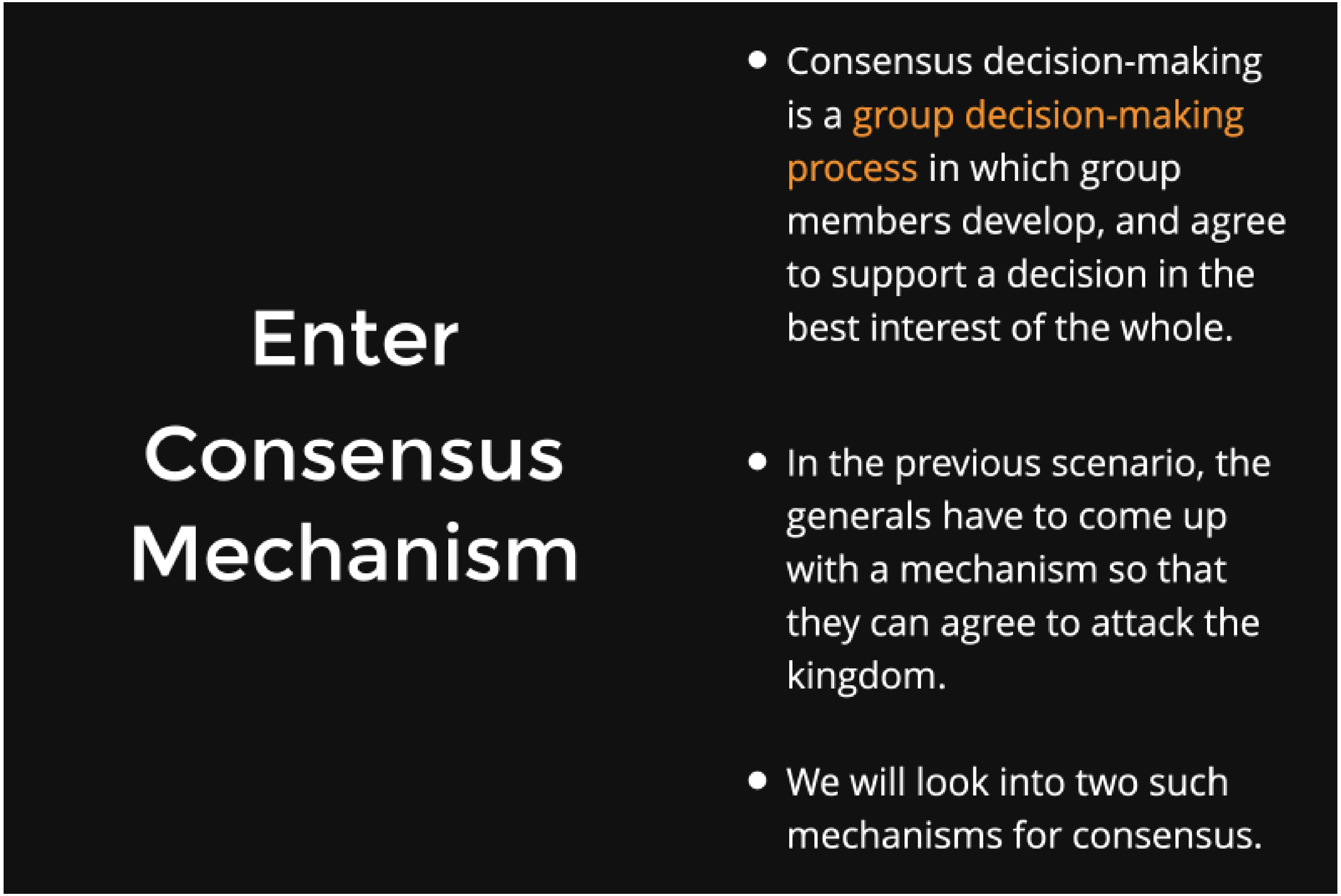
'Cause nothing comes without work

Byzantine Generals Problem



Coordinated Attack Leading to Victory

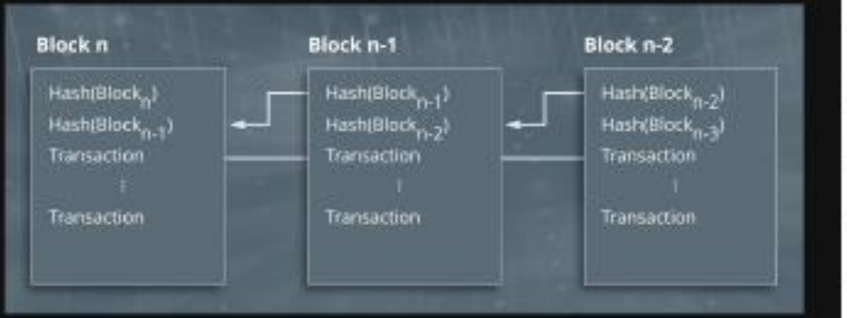
Uncoordinated Attack Leading to Defeat



Enter Consensus Mechanism

- Consensus decision-making is a group decision-making process in which group members develop, and agree to support a decision in the best interest of the whole.
- In the previous scenario, the generals have to come up with a mechanism so that they can agree to attack the kingdom.
- We will look into two such mechanisms for consensus.

What is a block?



Block n

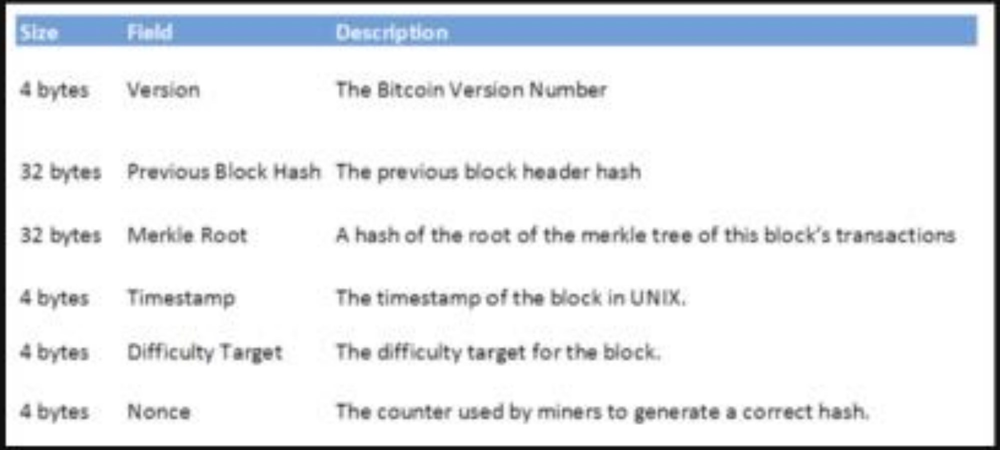
Hash(Block$_{n}$)
Hash(Block$_{n-1}$)
Transaction
⁞
Transaction

Block n-1

Hash(Block$_{n-1}$)
Hash(Block$_{n-2}$)
Transaction
⁞
Transaction

Block n-2

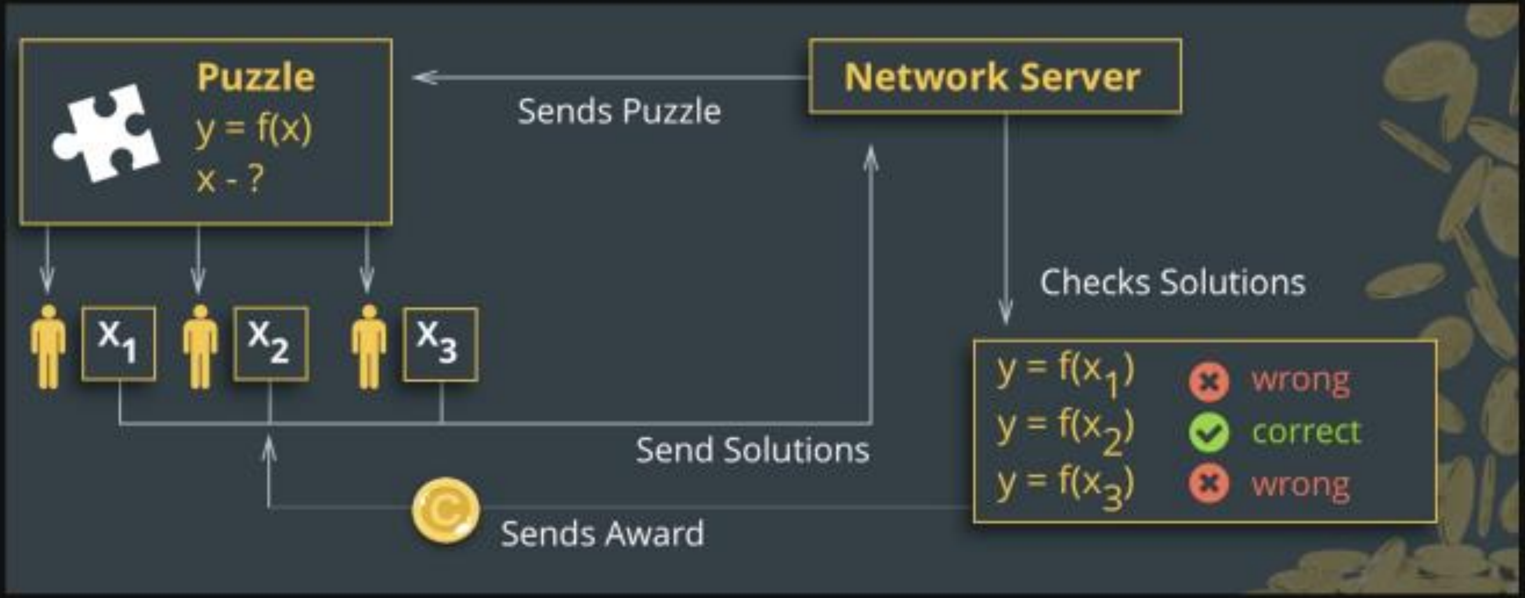
Hash(Block$_{n-2}$)
Hash(Block$_{n-3}$)
Transaction
⁞
Transaction



Size	Field	Description
4 bytes	Version	The Bitcoin Version Number
32 bytes	Previous Block Hash	The previous block header hash
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The timestamp of the block in UNIX.
4 bytes	Difficulty Target	The difficulty target for the block.
4 bytes	Nonce	The counter used by miners to generate a correct hash.

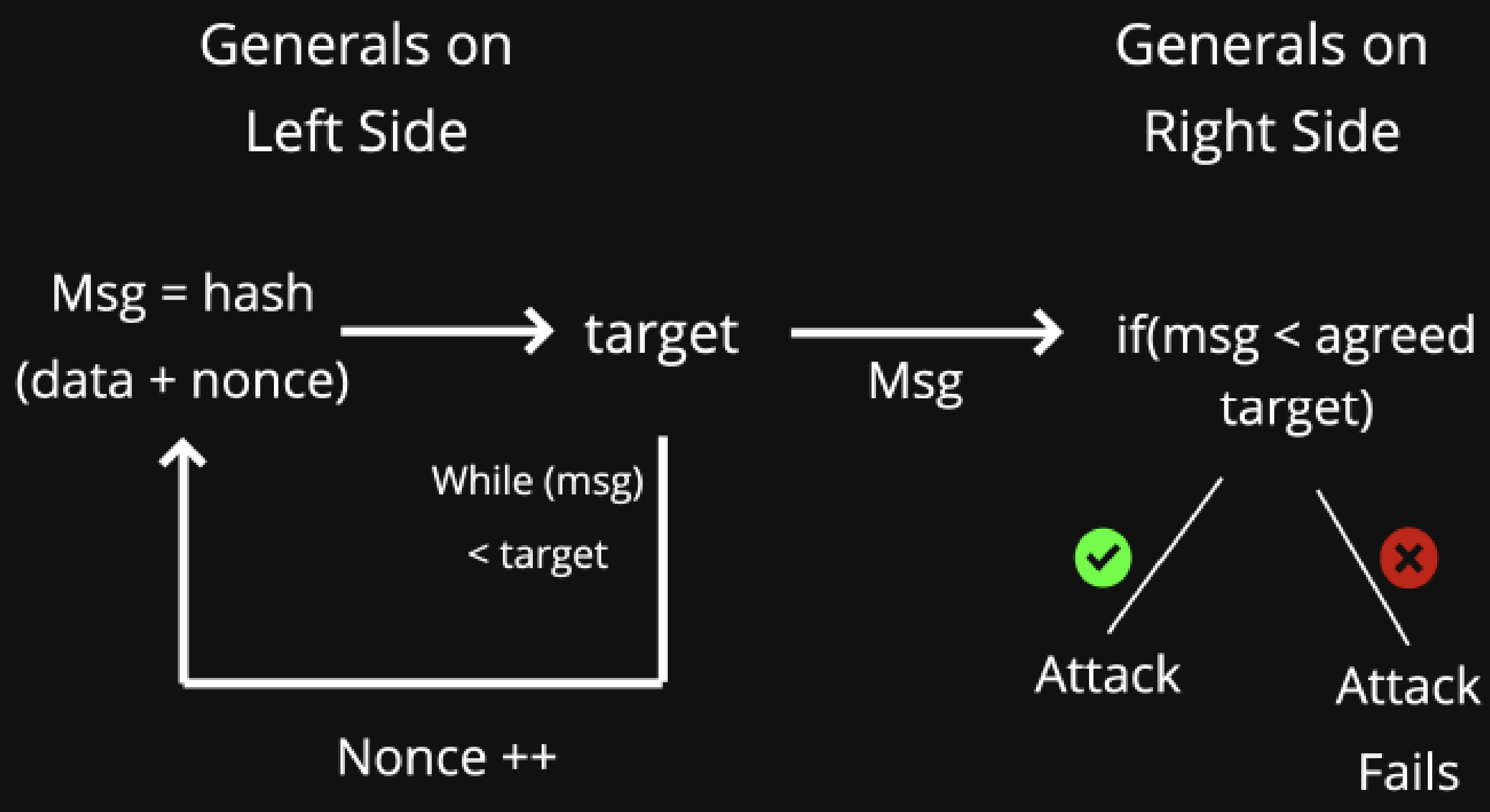
- A block is a group of transactions in chronological order (or the best chronological order that the miner nodes can agree and organize the transactions in).
- **Every block has, as its data, the hash of the previous block. Each block is made of a Block Header and a "Block Body."**

Miner



- In terms of Proof of Work, a miner is a node which does the work, validates the transaction and then creates the block which will then be appended to the blockchain.
- The miner receives block reward as an incentive for validating transactions and adding new blocks thus effectively maintaining the network.

Proof of Work



Generals on
Left Side

Generals on
Right Side

Msg = hash
(data + nonce)

target

Msg

if(msg < agreed
target)

While (msg)
< target

Nonce ++

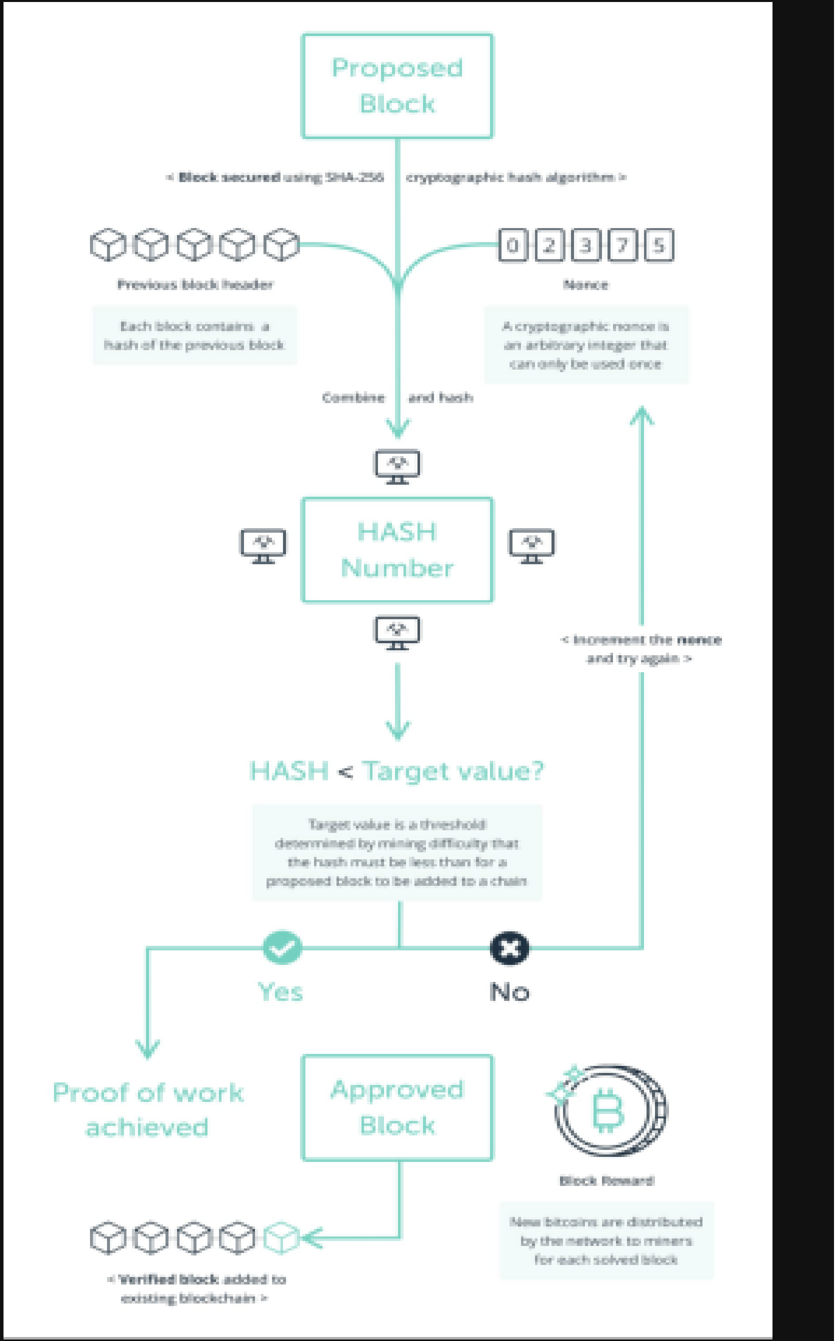
✓ Attack

✗ Attack
Fails

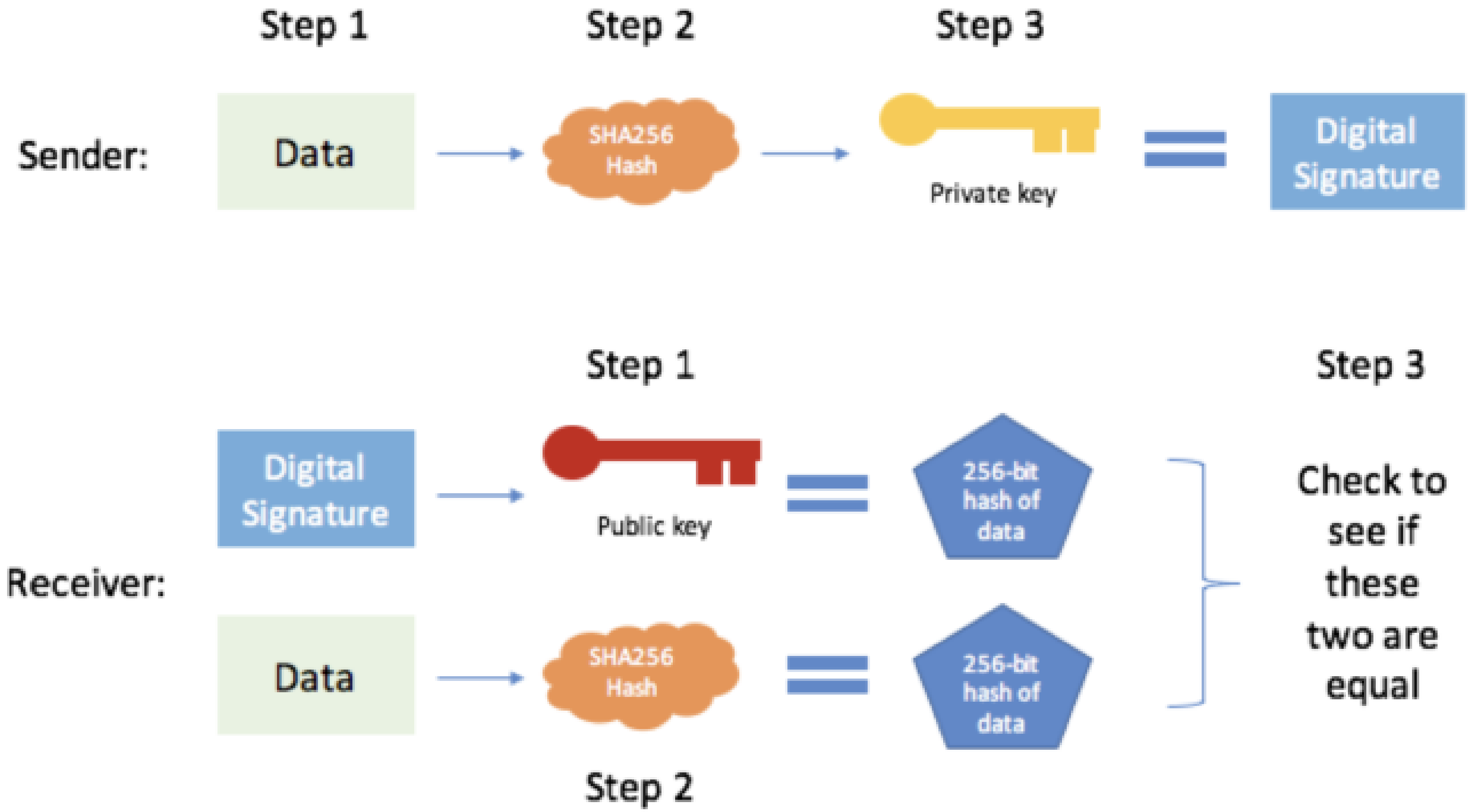
PoW Steps

- The algorithm works in such a way that it's difficult to generate the hash i.e. do the work but it's relatively easy to validate the hash.

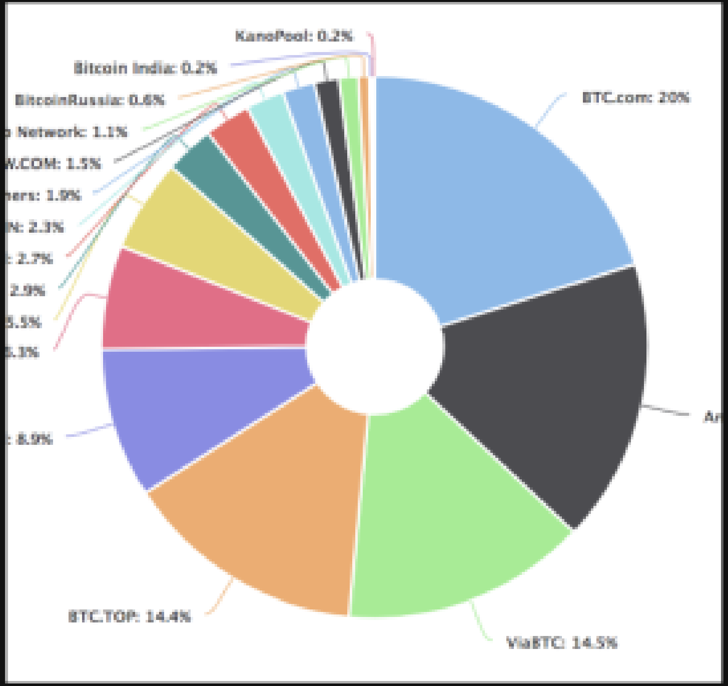
- The target value is determined by the difficulty which is set by the algorithm and is updated dynamically to not make it easier to add blocks to the chain.


Proposed Block
< Block secured using SHA-256 cryptographic hash algorithm >
Previous block header
Each block contains a hash of the previous block
0 2 3 7 5
Nonce
A cryptographic nonce is an arbitrary integer that can only be used once
Combine and hash
HASH Number
< Increment the nonce and try again >
HASH < Target value?
Target value is a threshold determined by mining difficulty that the hash must be less than for a proposed block to be added to a chain
Yes
No
Proof of work achieved
Approved Block
Block Reward
New bitcoins are distributed by the network to miners for each solved block
< Verified block added to existing blockchain >

Verification



PoW Cons



- Extensive utilization of computation resources for nothing other than calculating hashes.

- In a typical scenario, mining can be done either individually or by collectively mining using a pool. In time 2-3 of these pools could be so big that they could carry out a 51% attack themselves.

Proof of Stake

'Cause money brings trust

What is Proof of Stake??

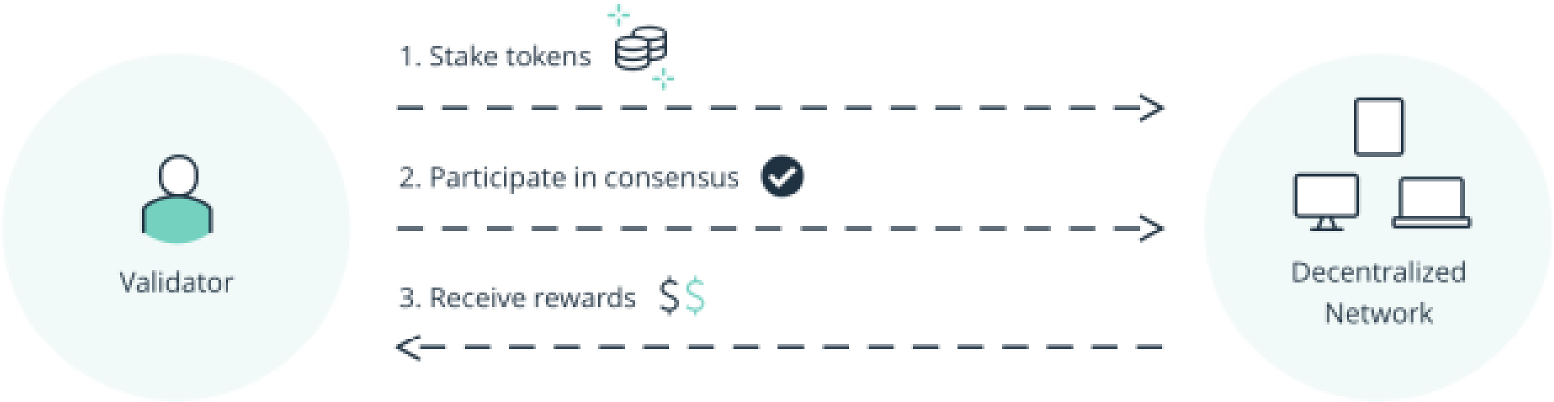
Proof of stake

The probability of validating a new block is determined by how large of a stake a person hold.

The validators do not receive a block reward, instead they collect network fees as their reward.

Proof of stake systems can be much more cost and energy efficient than proof of work, but are less proven.

Validator… who art thou



- Validators are selected randomly based on the stake they put forward.
- Their role is to validate the transactions and create a new block, which will then be submitted to the network for verification. Upon the verification if block gets added, validator will get reward.

How are validators selected?

- Randomized Block Selection: Validators are selected with the lowest hash value and highest stake.
- Coin Age solution: Validators are chosen based on how long their tokens have been staked for.

PoS... Cons...

- Proof of stake comes nowhere near to the adoption level of Proof of Work. Proof of work has seen millions of transactions in various blockchains. So it remains to be seen if it can be used in a scalable way to achieve consensus.
- Essentially, the more the stake the better the chance of getting selected to forge a block.

Consensus Models

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Round Robin
- Proof of Authority/Proof of Identity
- Proof of Elapsed Time (PoET)
- ….

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Stake (PoS)

- The proof of stake (PoS) model is based on the idea that the more stake a user has invested into the system, the more likely they will want the system to succeed, and the less likely they will want to subvert it.
- Stake is often an amount of cryptocurrency that the blockchain network user has invested into the system (through various means, such as by locking it via a special transaction type, or by sending it to a specific address, or holding it within special wallet software).
- Once staked, the cryptocurrency is generally no longer able to be spent.
- Proof of stake blockchain networks use the amount of stake a user has as a determining factor for publishing new blocks.
- Thus, the likelihood of a blockchain network user publishing a new block is tied to the ratio of their stake to the overall blockchain network amount of staked cryptocurrency.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Stake (PoS)

- With this consensus model, there is no need to perform resource intensive computations (involving time, electricity, and processing power) as found in proof of work.
- The methods for how the blockchain network uses the stake can vary.
  - random selection of staked users
  - multi-round voting
  - coin aging systems
  - delegate systems.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Stake (PoS) – Random selection of staked users

- When the choice of block publisher is a random choice (sometimes referred to as *chain-based proof of stake*), 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.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Stake (PoS) – Multi-round voting

- When the choice of block publisher is a multi-round voting system (sometime referred to as *Byzantine fault tolerance proof of stake*) there is added complexity.
- 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.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Stake (PoS) – Coin aging systems

- When the choice of block publisher is through a coin age system referred to as a *coin age proof of stake,* staked cryptocurrency has an *age* property.
- After a certain amount of time (such as 30 days) 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.
- This method allows for users with more stake to publish more blocks, but to not dominate the system – since they have a cooldown timer attached to every cryptocurrency coin *counted* towards creating blocks.
- Older coins and larger groups of coins will increase the probability of being chosen to publish the next block.
- To prevent stakeholders from hoarding aged cryptocurrencies, there is generally a built-in maximum to the probability of winning.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Stake (PoS) - delegate systems

- When the choice of block publisher is through a delegate system, users vote for nodes to become publishing nodes – therefore creating blocks on their behalf.
- Blockchain network users' voting power is tied to their stake so the larger the stake, the more weight the vote has.
- Nodes who receive the most votes become publishing nodes and can validate and publish blocks.
- Blockchain network users can also vote against an established publishing node, to try to remove them from the set of publishing nodes.
- Voting for publishing nodes is continuous and remaining a publishing node can be quite competitive.
- The threat of losing publishing node status, and therefore rewards and reputation is constant so publishing nodes are incentivized to not act maliciously.
- Additionally, blockchain network users vote for delegates, who participate in the governance of the blockchain.
- Delegates will propose changes, and improvements, which will be voted on by blockchain network users.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Round Robin Consensus Model

- Round Robin is a consensus model that is used by some permissioned blockchain networks.
- Within this model of consensus, nodes take turns in creating blocks.
- To handle situations where a publishing node is not available to publish a block on its turn, these systems may include a time limit to enable available nodes to publish blocks so that unavailable nodes will not cause a halt in block publication.
- This model ensures no one node creates the majority of the blocks.
- It benefits from a straightforward approach, lacks cryptographic puzzles, and has low power requirements.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Round Robin Consensus Model

- Since there is a need for trust amongst nodes, round robin does not work well in the permissionless blockchain networks used by most cryptocurrencies.
- This is because malicious nodes could continuously add additional nodes to increase their odds of publishing new blocks.
- In the worst case, they could use this to subvert the correct operation of the blockchain network.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Authority/Proof of Identity

- The proof of authority (also referred to as proof of identity) consensus model relies on the partial trust of publishing nodes through their known link to real world identities.
- Publishing nodes must have their identities proven and verifiable within the blockchain network (e.g., identifying documents which have been verified and notarized and included on the blockchain).
- The idea is that the publishing node is staking its identity/ reputation to publish new blocks.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Authority/Proof of Identity

- Blockchain network users directly affect a publishing node’s reputation based on the publishing node’s behavior.
- Publishing nodes can lose reputation by acting in a way that the blockchain network users disagree with, just as they can gain reputation by acting in a manner that the blockchain network users agree with.
- The lower the reputation, the less likelihood of being able to publish a block. Therefore, it is in the interest of a publishing node to maintain a high reputation.
- This algorithm only applies to permissioned blockchain networks with high levels of trust.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Elapsed Time Consensus

- Within the proof of elapsed time (PoET) consensus model, each publishing node requests a wait time from a secure hardware time source within their computer system.
- The secure hardware time source will generate a random wait time and return it to the publishing node software.
- Publishing nodes take the random time they are given and become idle for that duration.
- Once a publishing node wakes up from the idle state, it creates and publishes a block to the blockchain network, alerting the other nodes of the new block; any publishing node that is still idle will stop waiting, and the entire process starts over.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Elapsed Time Consensus

- This model requires ensuring that a random time was used, since if the time to wait was not selected at random a malicious publishing node would just wait the minimum amount of time by default to dominate the system.
- This model also requires ensuring that the publishing node waited the actual time and did not start early.
- These requirements are being solved by executing software in a trusted execution environment found on some computer processors (such as Intel’s Software Guard Extensions, or AMD’s Platform Security Processor, or ARM’s TrustZone).

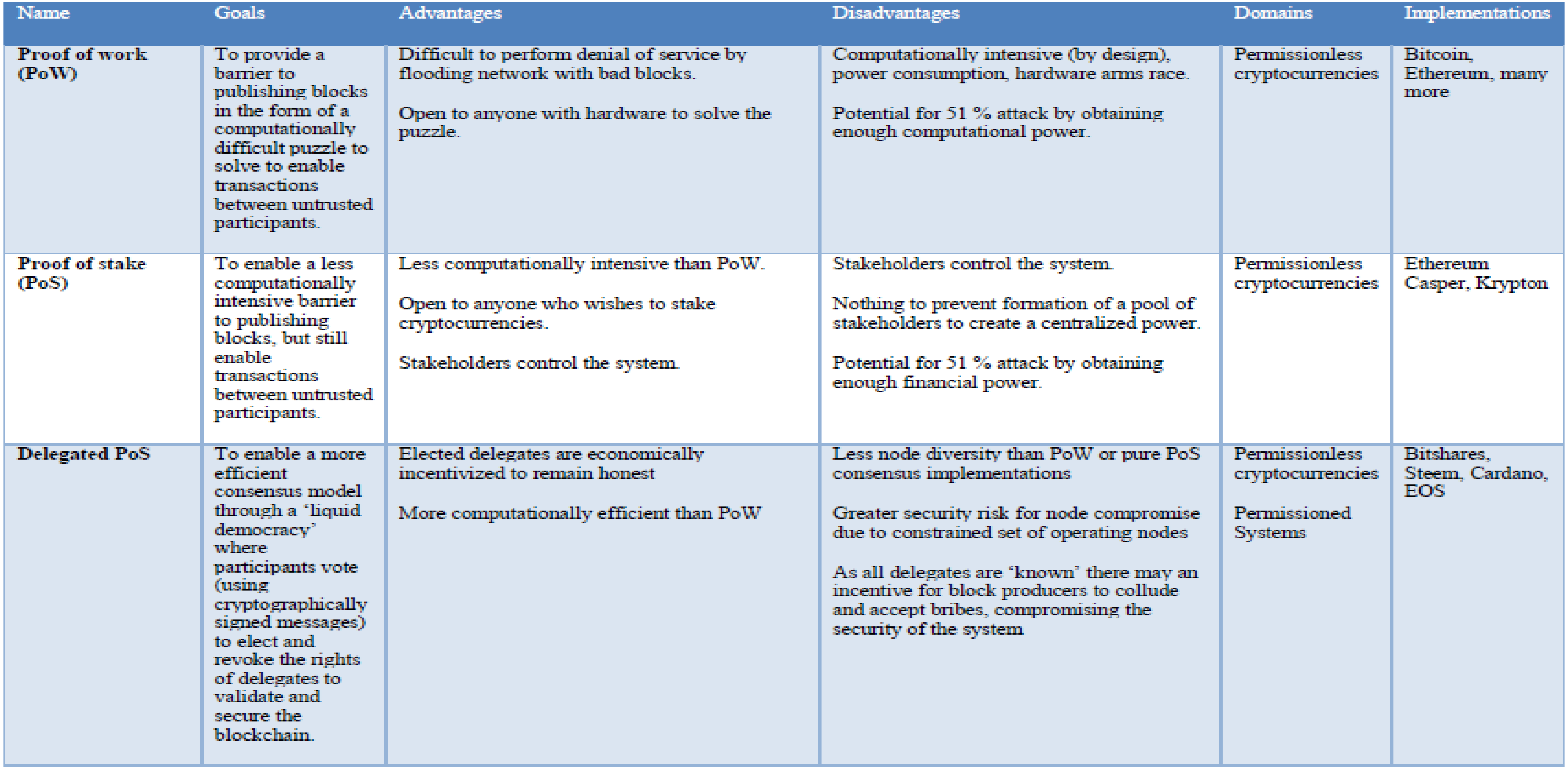
Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Proof of Elapsed Time Consensus

- Verified and trusted software can run in these secure execution environments and cannot be altered by outside programs.
- A publishing node would query software running in this secure environment for a random time and then wait for that time to pass.
- After waiting the assigned time, the publishing node could request a signed certificate that the publishing node waited the randomly assigned time.
- The publishing node then publishes the certificate along with the block.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

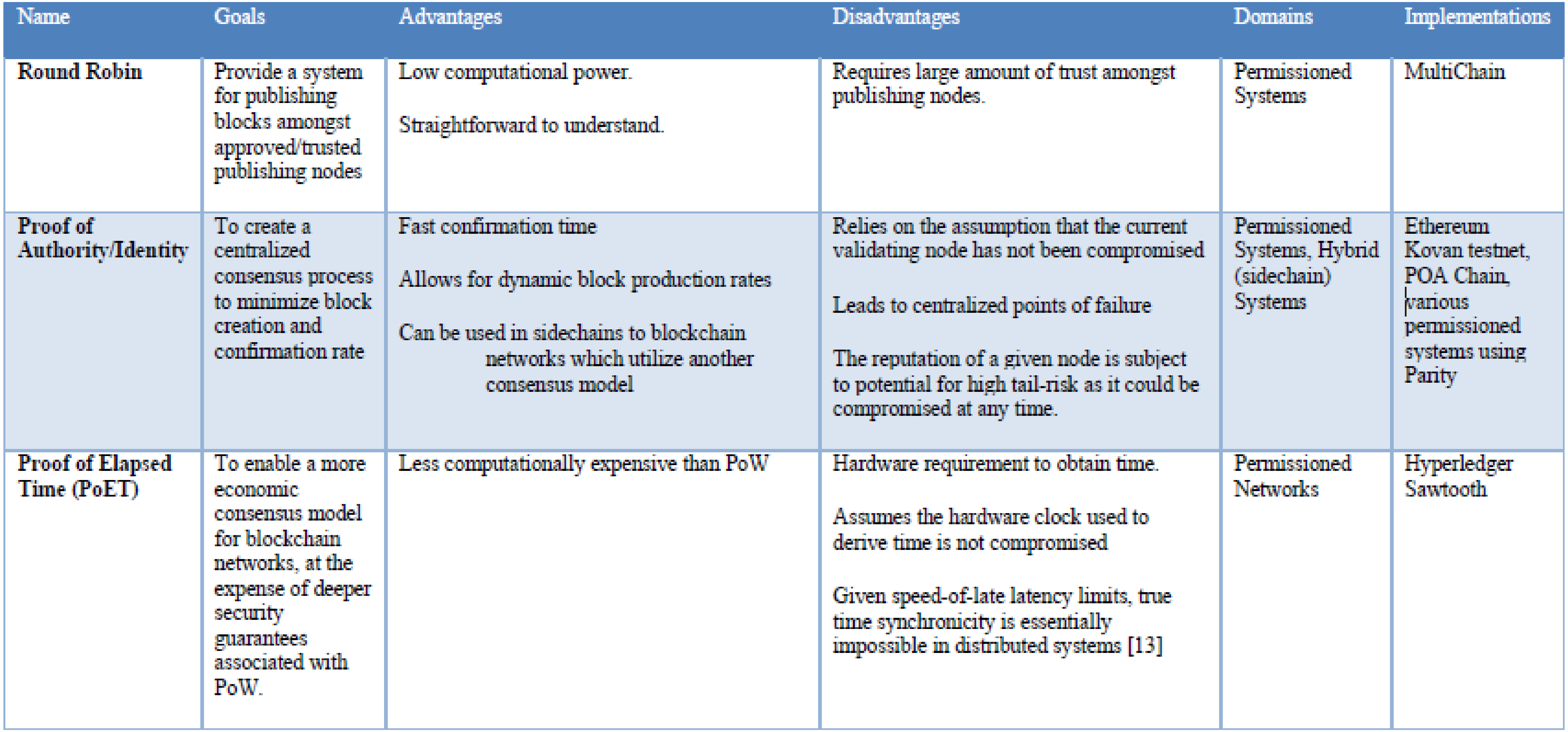
Comparison of Consensus models



Name	Goals	Advantages	Disadvantages	Domains	Implementations
Proof of work (PoW)	To provide a barrier to publishing blocks in the form of a computationally difficult puzzle to solve to enable transactions between untrusted participants.	Difficult to perform denial of service by flooding network with bad blocks. Open to anyone with hardware to solve the puzzle.	Computationally intensive (by design), power consumption, hardware arms race. Potential for 51 % attack by obtaining enough computational power.	Permissionless cryptocurrencies	Bitcoin, Ethereum, many more
Proof of stake (PoS)	To enable a less computationally intensive barrier to publishing blocks, but still enable transactions between untrusted participants.	Less computationally intensive than PoW. Open to anyone who wishes to stake cryptocurrencies. Stakeholders control the system.	Stakeholders control the system. Nothing to prevent formation of a pool of stakeholders to create a centralized power. Potential for 51 % attack by obtaining enough financial power.	Permissionless cryptocurrencies	Ethereum Casper, Krypton
Delegated PoS	To enable a more efficient consensus model through a 'liquid democracy' where participants vote (using cryptographically signed messages) to elect and revoke the rights of delegates to validate and secure the blockchain.	Elected delegates are economically incentivized to remain honest More computationally efficient than PoW	Less node diversity than PoW or pure PoS consensus implementations Greater security risk for node compromise due to constrained set of operating nodes As all delegates are 'known' there may an incentive for block producers to collude and accept bribes, compromising the security of the system	Permissionless cryptocurrencies Permissioned Systems	Bitshares, Steem, Cardano, EOS

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Comparison of Consensus models



Name	Goals	Advantages	Disadvantages	Domains	Implementations
Round Robin	Provide a system for publishing blocks amongst approved/trusted publishing nodes	Low computational power. Straightforward to understand.	Requires large amount of trust amongst publishing nodes.	Permissioned Systems	MultiChain
Proof of Authority/Identity	To create a centralized consensus process to minimize block creation and confirmation rate	Fast confirmation time Allows for dynamic block production rates Can be used in sidechains to blockchain networks which utilize another consensus model	Relies on the assumption that the current validating node has not been compromised Leads to centralized points of failure The reputation of a given node is subject to potential for high tail-risk as it could be compromised at any time.	Permissioned Systems, Hybrid (sidechain) Systems	Ethereum Kovan testnet, POA Chain, various permissioned systems using Parity
Proof of Elapsed Time (PoET)	To enable a more economic consensus model for blockchain networks, at the expense of deeper security guarantees associated with PoW.	Less computationally expensive than PoW	Hardware requirement to obtain time. Assumes the hardware clock used to derive time is not compromised Given speed-of-late latency limits, true time synchronicity is essentially impossible in distributed systems [13]	Permissioned Networks	Hyperledger Sawtooth

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Forking

- Soft forks
- Hard forks

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Soft Fork

- A *soft fork* is a change to a blockchain implementation that is backwards compatible.
- Non-updated nodes can continue to transact with updated nodes.
- If no (or very few) nodes upgrade, then the updated rules will not be followed.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Soft Fork

- An example of a soft fork occurred on Bitcoin when a new rule was added to support escrow.
- 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 [8] and time-locked refunds.
- In 2014, a proposal was made to repurpose an operation code that performed no operation (OP_NOP2) to CHECKLOCKTIMEVERIFY, which allows a transaction output to be made spendable at a point in the future had been executed.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Soft Fork

- A fictional example of a soft fork would be if a blockchain decided to reduce the size of blocks (for example from 1.0 MB to 0.5 MB).
- Updated nodes would adjust the block size and continue to transact as normal;
- non-updated nodes would see these blocks as valid – since the change made does not violate their rules (i.e., the block size is under their maximum allowed).
- However, if a non-updated node were to create a block with a size greater than 0.5 MB, updated nodes would reject them as invalid.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Hard Fork

- A *hard fork* is a change to a blockchain implementation that is not backwards compatible.
- At a given point in time (usually at a specific block number), all publishing nodes will need to switch to using the updated protocol.
- Additionally, all nodes will need to upgrade to the new protocol so that they do not reject the newly formatted blocks.
- 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.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Hard Fork

- A well-known example of a hard fork is from Ethereum.
- In 2016, a smart contract was constructed on Ethereum called the Decentralized Autonomous Organization (DAO).
- Due to flaws in how the smart contract was constructed, an attacker extracted Ether, the cryptocurrency used by Ethereum, resulting in the theft of $50 million.
- A hard fork proposal was voted on by Ether holders, and the clear majority of users agreed to hard fork and create a new version of the blockchain, without the flaw, and that also returned the stolen funds.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Hard Fork

- With cryptocurrencies, if there is a hard fork and the blockchain splits then users will have independent currency on both forks (having double the number of coins in total).
- If all the activity moves to the new chain, the old one may eventually not be used since the two chains are not compatible (they will be independent currency systems).
- In the case of the Ethereum hard fork, the clear majority of support moved to the new fork, the old fork was renamed Ethereum Classic and continued operating.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Smart contracts

- The term smart contract dates to 1994, defined by Nick Szabo as “a computerized transaction protocol that executes the terms of a contract.
- The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries.”

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Smart contracts

- Smart contracts extend and leverage blockchain technology.
- A *smart contract* is a collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network (e.g., Ethereum’s smart contracts, Hyperledger Fabric’s chaincode).
- The smart contract is executed by nodes within the blockchain network;
- all nodes that execute the smart contract must derive the same results from the execution, and the results of execution are recorded on the blockchain.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Smart contracts

- The code, being on the blockchain, is also tamper evident and tamper resistant and therefore can be used (among other purposes) as a trusted third party.

- A smart contract can perform calculations, store information, expose properties to reflect a publicly exposed state and, if appropriate, automatically send funds to other accounts.

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Smart contracts

- For smart contract enabled permissionless blockchain networks (such as Ethereum) the user issuing a transaction to a smart contract will have to pay for the cost of the code execution.
- There is a limit on how much execution time can be consumed by a call to a smart contract, based on the complexity of the code.
- If this limit is exceeded, execution stops, and the transaction is discarded.
- This mechanism not only rewards the publishers for executing the smart contract code, but also prevents malicious users from deploying and then accessing smart contracts that will perform a denial of service on the publishing nodes by consuming all resources (e.g., using infinite loops).

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

Smart contracts

- For smart contract enabled permissioned blockchain networks, such as those utilizing Hyperledger Fabric’s chaincode, there may not be a requirement for users to pay for smart contract code execution.
- These networks are designed around having known participants, and other methods of preventing bad behavior can be employed (e.g., revoking access).

Source : Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

What Is Cryptocurrency?

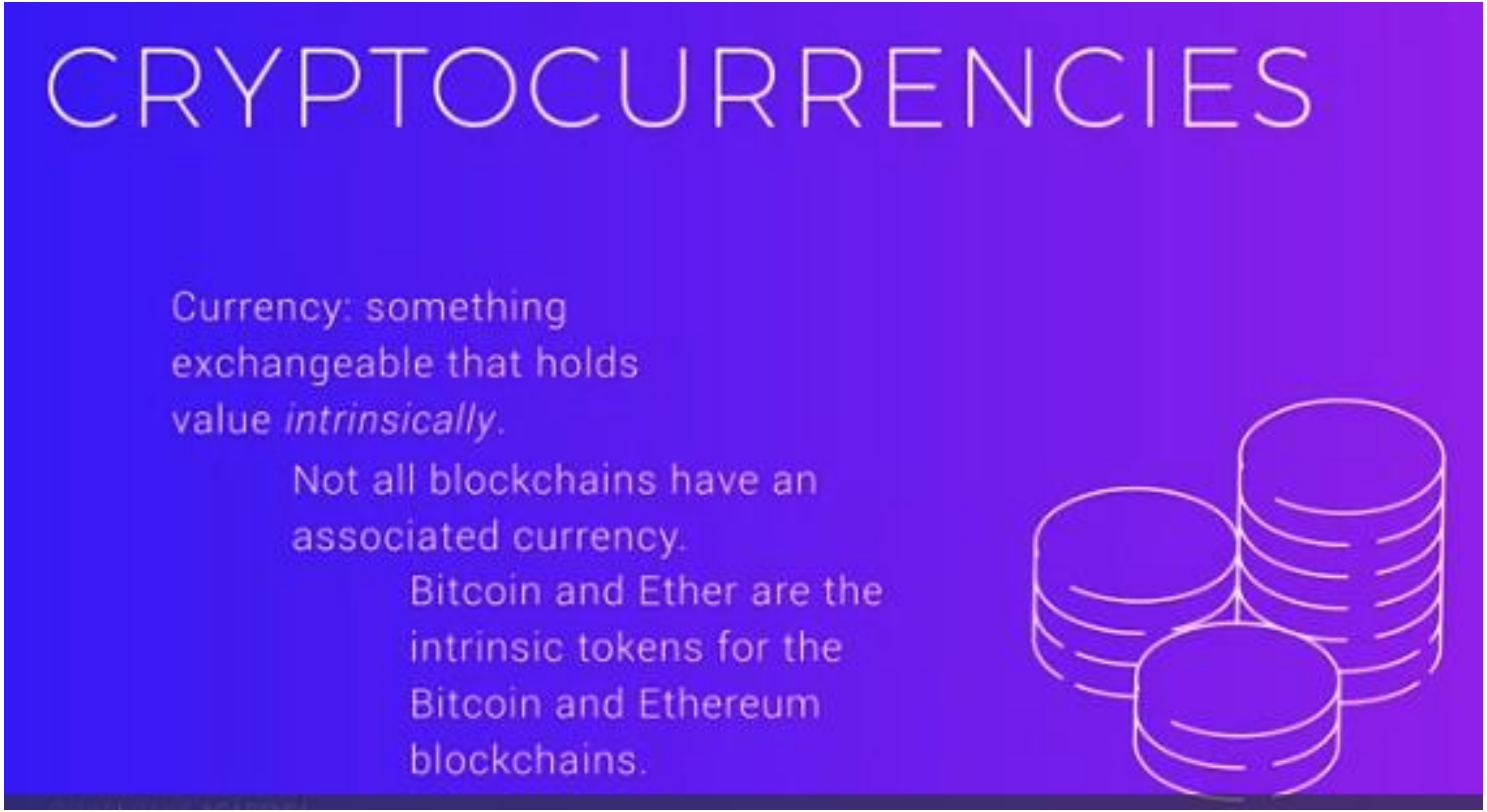
- A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend.

- Many cryptocurrencies are decentralized networks based on blockchain technology—a distributed ledger enforced by a disparate network of computers.

- A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.

What Is Cryptocurrency?

- A cryptocurrency is a form of digital asset based on a network that is distributed across a large number of computers. This decentralized structure allows them to exist outside the control of governments and central authorities.
- The word “cryptocurrency” is derived from the encryption techniques which are used to secure the network.
- Blockchains, which are organizational methods for ensuring the integrity of transactional data, are an essential component of many cryptocurrencies.
- Cryptocurrencies face criticism for a number of reasons, including their use for illegal activities, exchange rate volatility, and vulnerabilities of the infrastructure underlying them.



CRYPTOCURRENCIES

Currency: something exchangeable that holds value *intrinsically*.

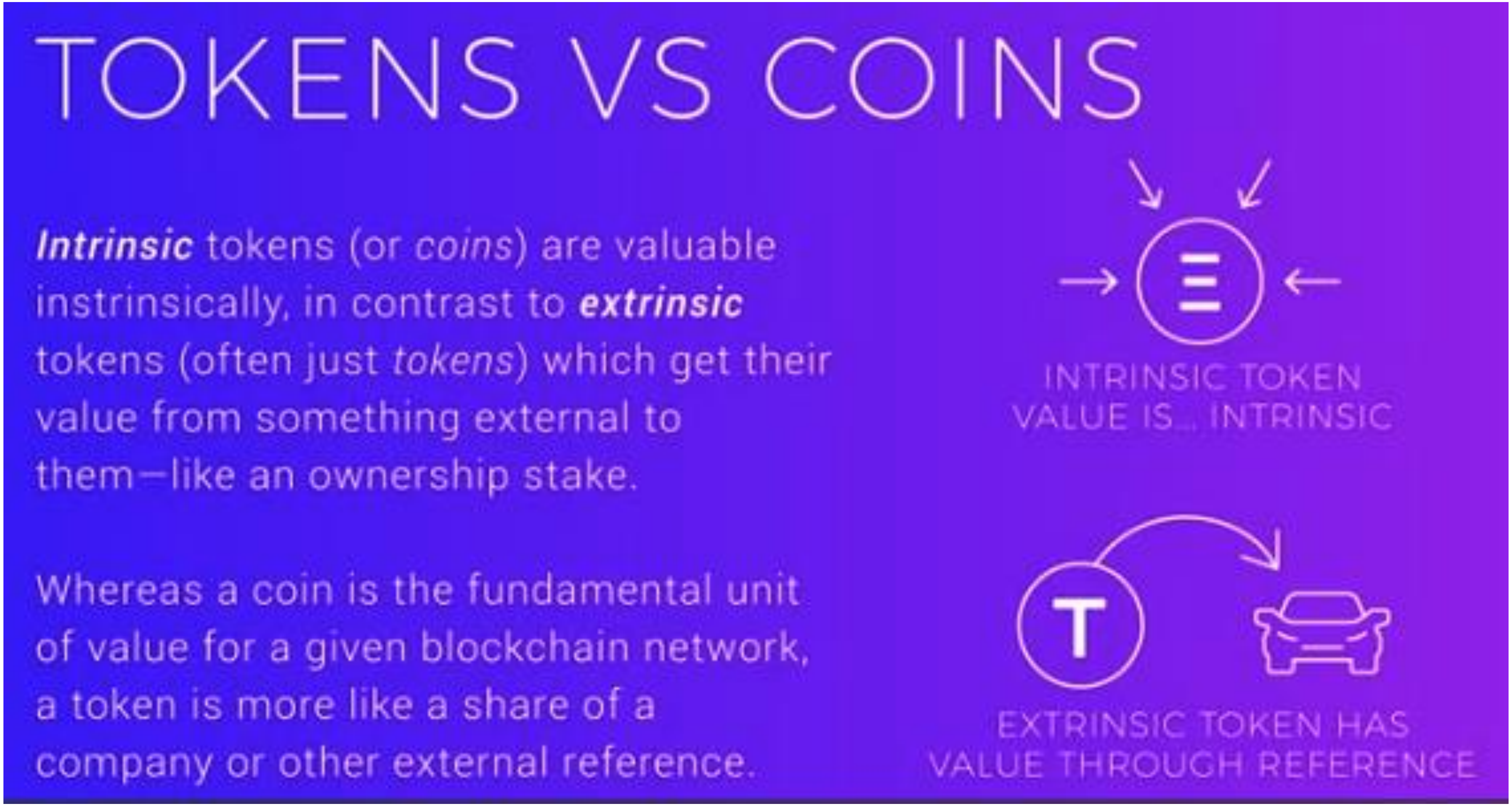
Not all blockchains have an associated currency.

Bitcoin and Ether are the intrinsic tokens for the Bitcoin and Ethereum blockchains.

Source : Coursera Course ‘Blockchain: Foundations and Use Cases’

What Are Crypto Tokens?

- Crypto tokens are a type of cryptocurrency that represents an asset or specific use and resides on their blockchain.
- Tokens can be used for investment purposes, to store value, or to make purchases.
- Cryptocurrencies are digital currencies used to facilitate transactions (making and receiving payments) along the blockchain.
- Altcoins and crypto tokens are types of cryptocurrencies with different functions.
- Created through an initial coin offering, crypto tokens are often used to raise funds for crowd sales.



TOKENS VS COINS

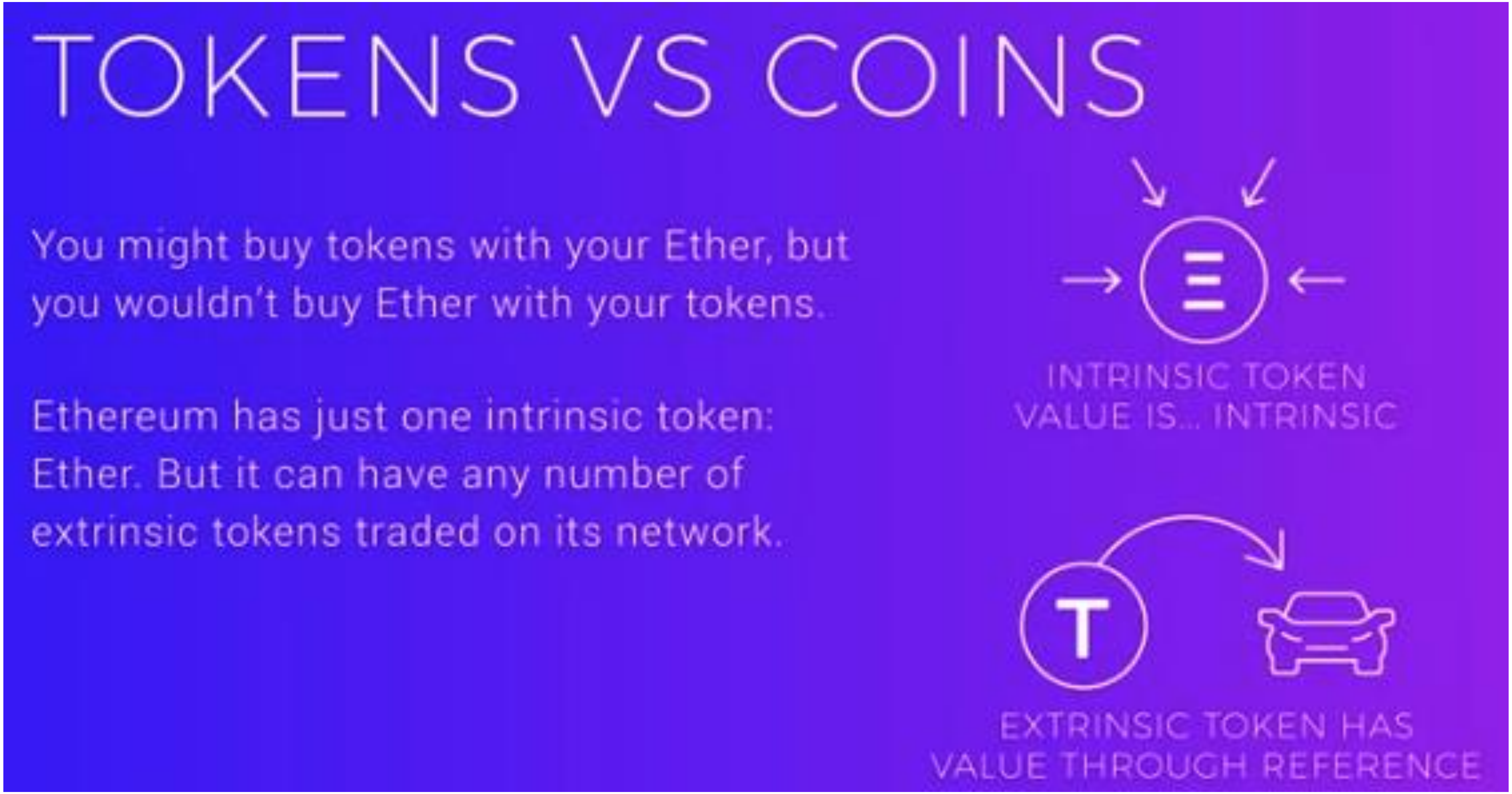
Intrinsic tokens (or *coins*) are valuable instrinsically, in contrast to ***extrinsic*** tokens (often just *tokens*) which get their value from something external to them—like an ownership stake.

Whereas a coin is the fundamental unit of value for a given blockchain network, a token is more like a share of a company or other external reference.

INTRINSIC TOKEN
VALUE IS… INTRINSIC

EXTRINSIC TOKEN HAS
VALUE THROUGH REFERENCE

Source : Coursera Course ‘Blockchain: Foundations and Use Cases’



TOKENS VS COINS

You might buy tokens with your Ether, but you wouldn't buy Ether with your tokens.

Ethereum has just one intrinsic token: Ether. But it can have any number of extrinsic tokens traded on its network.

Ξ
INTRINSIC TOKEN VALUE IS... INTRINSIC
T
EXTRINSIC TOKEN HAS VALUE THROUGH REFERENCE

Source : Coursera Course ‘Blockchain: Foundations and Use Cases’

What Is an ICO?

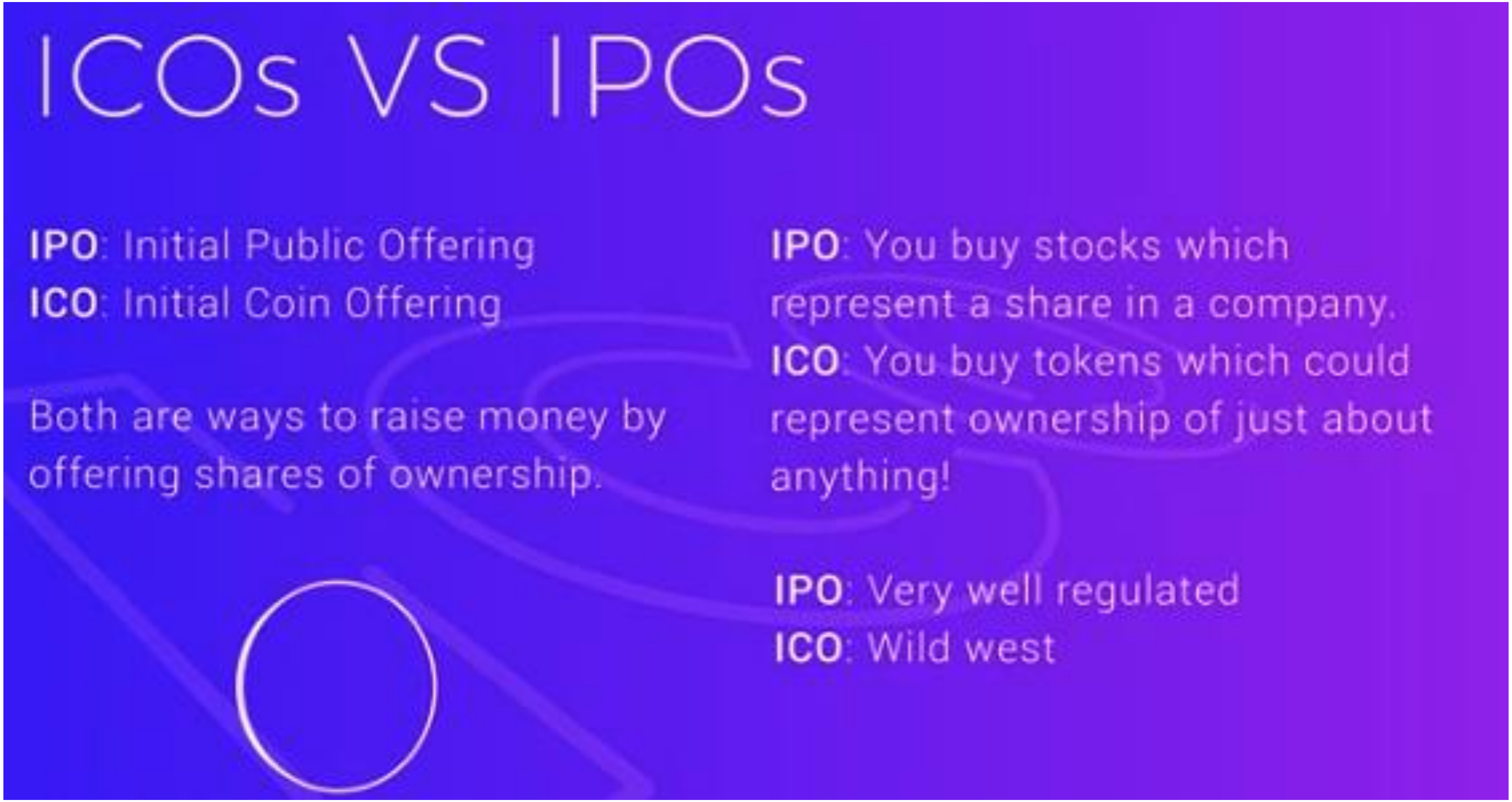
- Entrepreneurs looking to launch a new cryptocurrency can do it through an initial coin offering (ICO), a variation on an initial public offering (IPO).

- There is little to no government regulation of ICOs currently, and anyone can launch one, provided they get the technology put in place.

- How does one put the technology in place? Create a white paper or other document outlining the system, make a website or app describing how it works, and seek funding.

- Advertising is key since there are so many competing coins on the market, so figuring out how to appeal to the target demo is crucial.

- Not looking to launch a new coin, but rather, to invest in a new coin? Make sure to do thorough research, as there are a number of scams.



ICOs VS IPOs

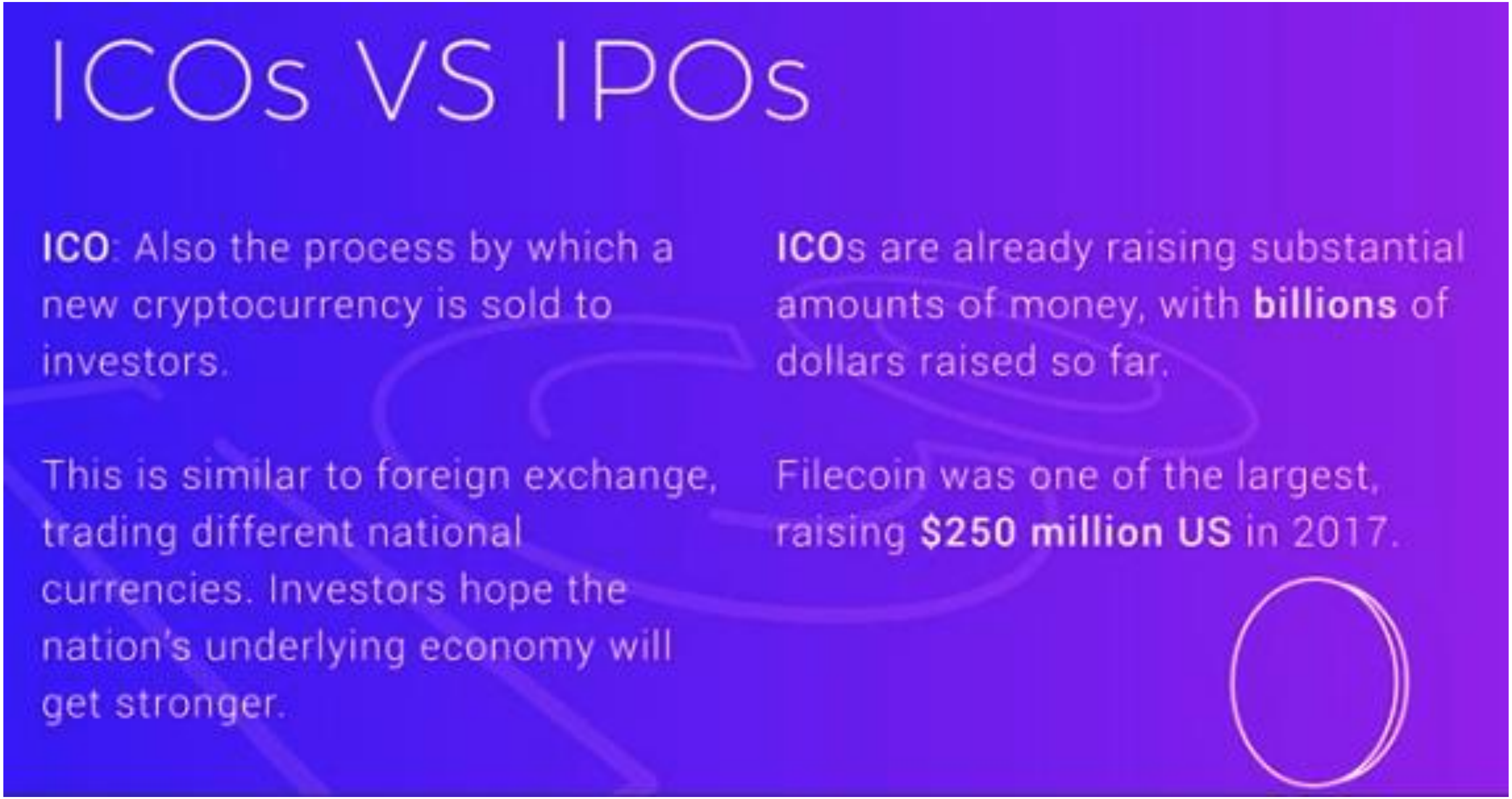
IPO: Initial Public Offering
ICO: Initial Coin Offering

Both are ways to raise money by offering shares of ownership.

IPO: You buy stocks which represent a share in a company.
ICO: You buy tokens which could represent ownership of just about anything!

IPO: Very well regulated
ICO: Wild west

Source : Coursera Course ‘Blockchain: Foundations and Use Cases’



ICOs VS IPOs

ICO: Also the process by which a new cryptocurrency is sold to investors.

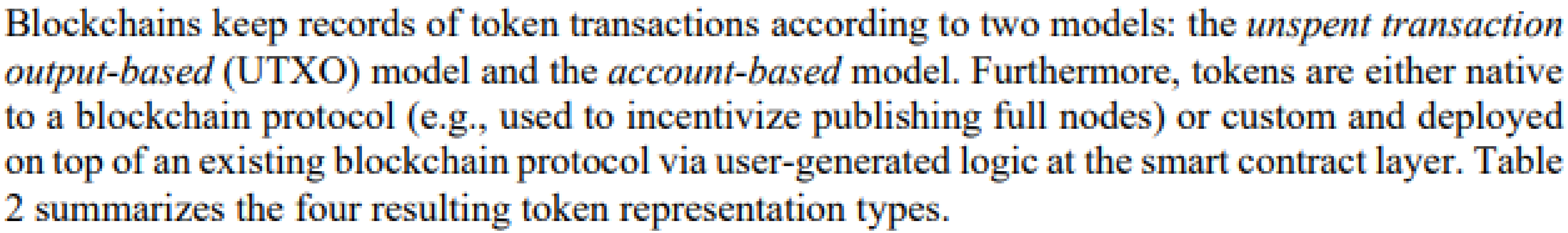
This is similar to foreign exchange, trading different national currencies. Investors hope the nation's underlying economy will get stronger.

ICOs are already raising substantial amounts of money, with **billions** of dollars raised so far.

Filecoin was one of the largest, raising **$250 million US** in 2017.

Source : Coursera Course ‘Blockchain: Foundations and Use Cases’

Token Data models

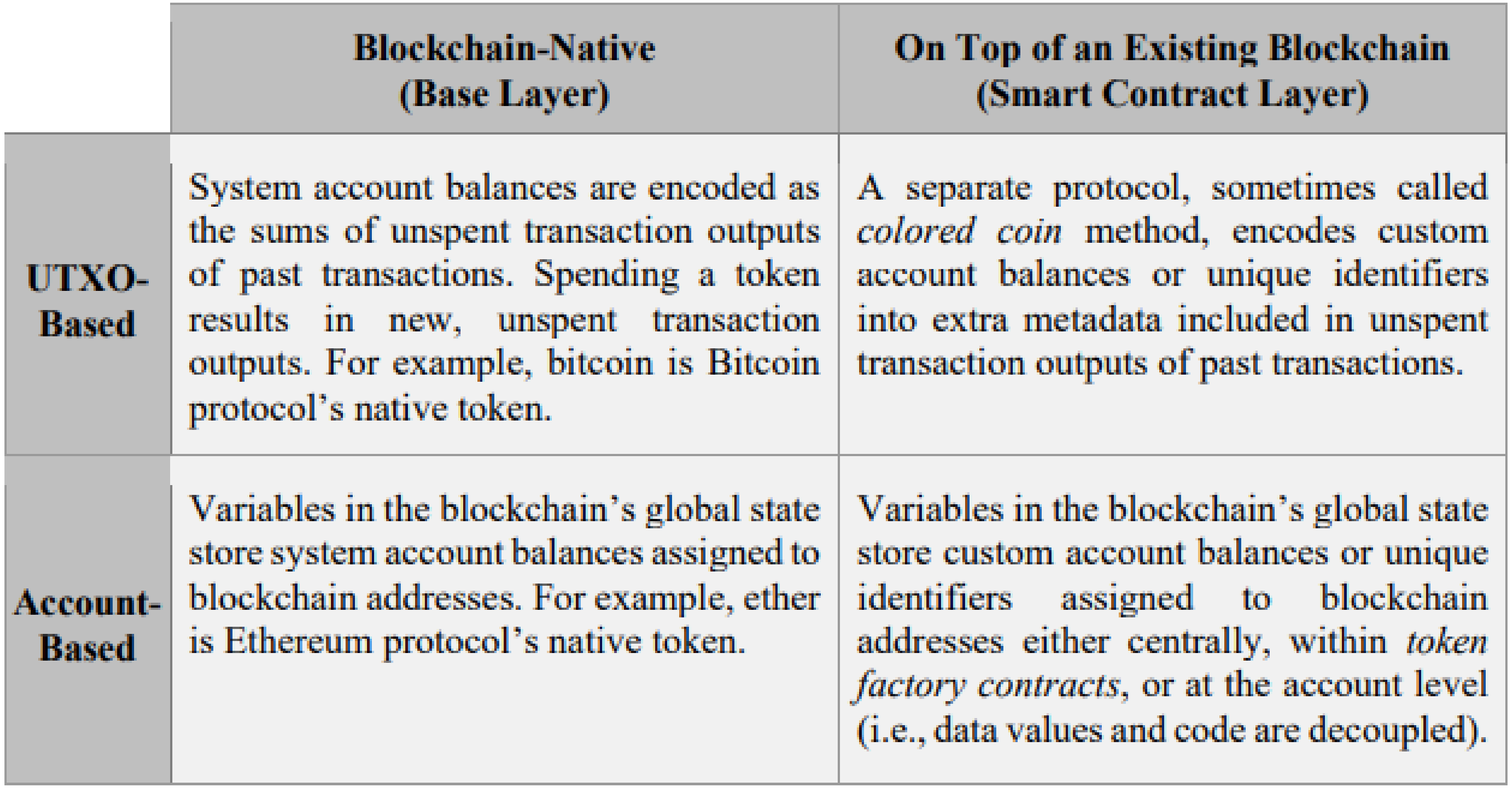


Blockchains keep records of token transactions according to two models: the *unspent transaction output-based* (UTXO) model and the *account-based* model. Furthermore, tokens are either native to a blockchain protocol (e.g., used to incentivize publishing full nodes) or custom and deployed on top of an existing blockchain protocol via user-generated logic at the smart contract layer. Table 2 summarizes the four resulting token representation types.

[Source : Lesavre, Loïc, Priam Varin, and Dylan Yaga. *Blockchain Networks: Token Design and Management Overview*. No. NIST Internal or Interagency Report (NISTIR) 8301 (Draft). National Institute of Standards and Technology, 2020.]

Token Data models

Table 2: Token Representation Types



	Blockchain-Native (Base Layer)	On Top of an Existing Blockchain (Smart Contract Layer)
UTXO-Based	System account balances are encoded as the sums of unspent transaction outputs of past transactions. Spending a token results in new, unspent transaction outputs. For example, bitcoin is Bitcoin protocol's native token.	A separate protocol, sometimes called *colored coin* method, encodes custom account balances or unique identifiers into extra metadata included in unspent transaction outputs of past transactions.
Account-Based	Variables in the blockchain's global state store system account balances assigned to blockchain addresses. For example, ether is Ethereum protocol's native token.	Variables in the blockchain's global state store custom account balances or unique identifiers assigned to blockchain addresses either centrally, within *token factory contracts*, or at the account level (i.e., data values and code are decoupled).

Source : Lesavre, Loïc, Priam Varin, and Dylan Yaga. *Blockchain Networks: Token Design and Management Overview*. No. NIST Internal or Interagency Report (NISTIR) 8301 (Draft). National Institute of Standards and Technology, 2020.