CHAPTER 1
BLOCKCHAIN 101

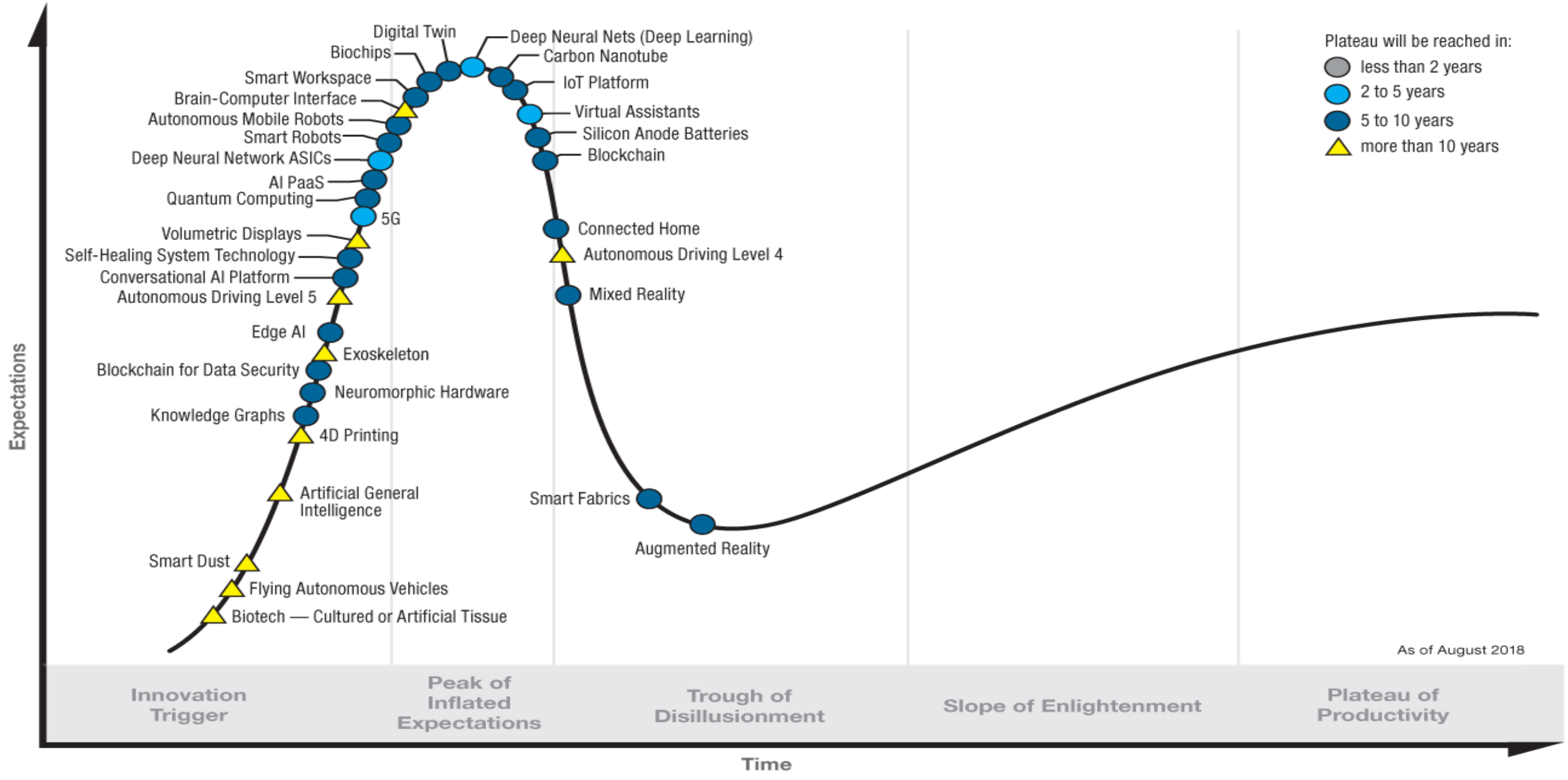
From : Mastering Blockchain

By – Imran Bashir

www.packet.com

Blockchain 101

Hype Cycle for Emerging Technologies, 2018



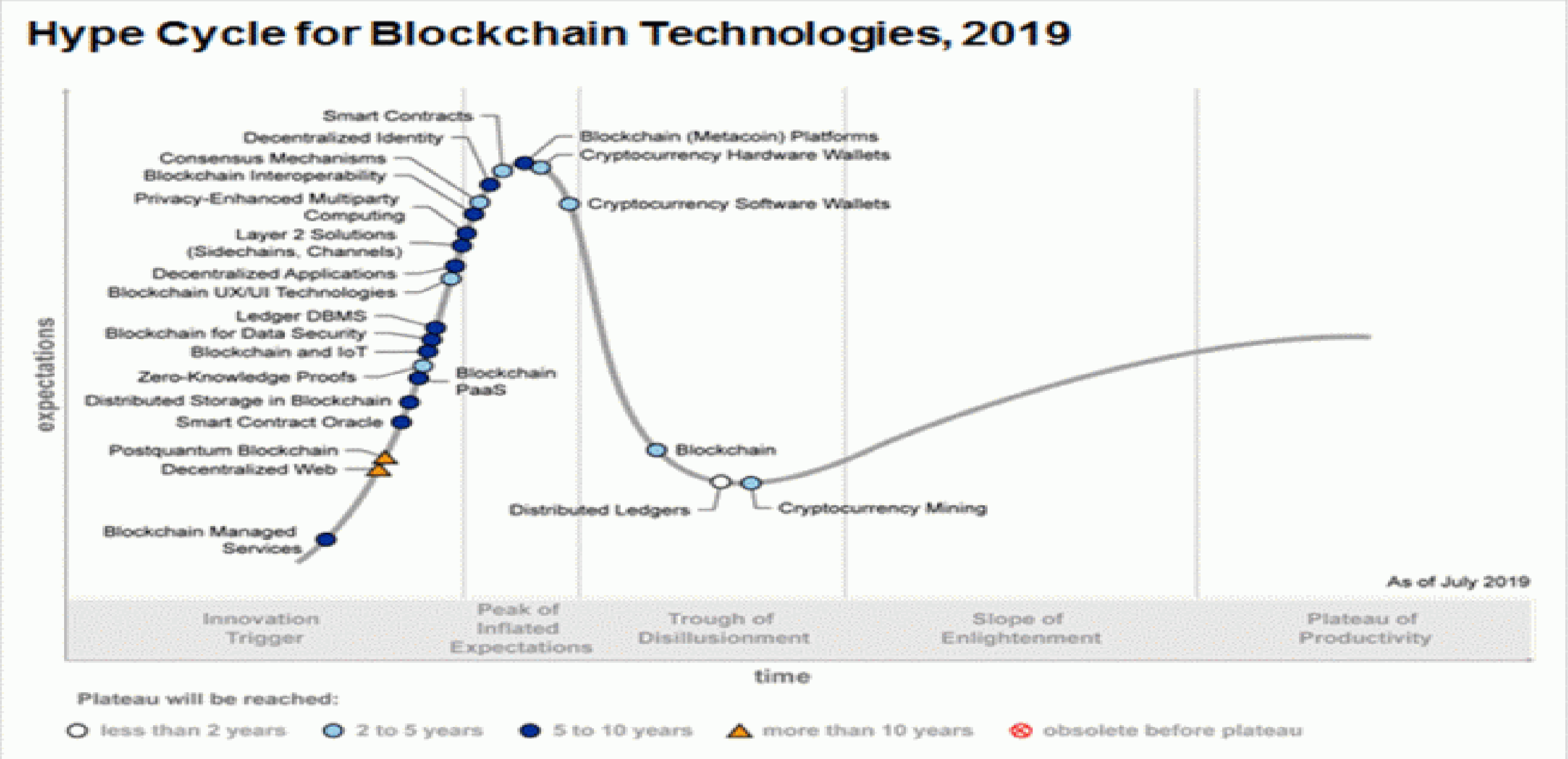
gartner.com/SmarterWithGartner

Source: Gartner (August 2018)

Gartner

Blockchain Technologies

Figure 1. Hype Cycle for Blockchain Technologies, 2019



Source: Gartner
ID: 383155

Birth Story

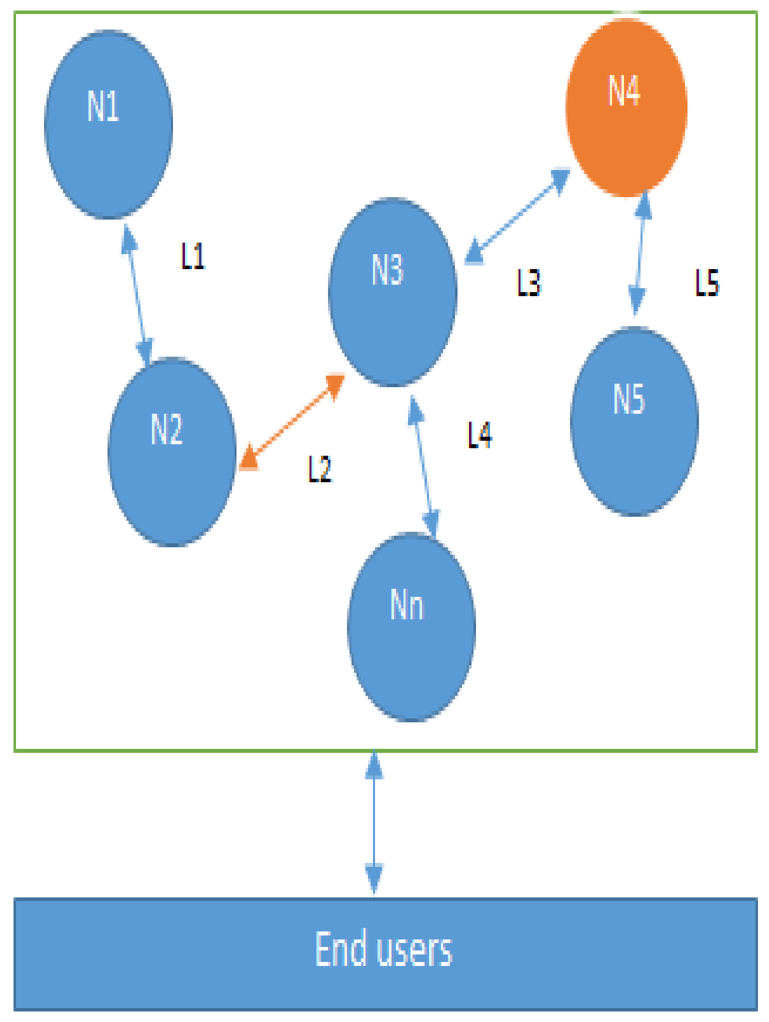
- In 2008 a ground breaking paper Bitcoin: A Peer-to-Peer Electronic Cash System was written on the topic of peer-to-peer electronic cash under the pseudonym Satoshi Nakamoto and introduced the term chain of blocks. This term over the years has now evolved into the word BLOCKCHAIN

Way to Understanding Blockchain

- This is a logical way of understanding blockchain technology because the roots of blockchain are in DISTRIBUTED SYSTEMS.

Distributed systems

- Distributed systems are a computing paradigm whereby two or more nodes work with each other in a coordinated fashion in order to achieve a common outcome and it's modelled in such a way that end users see it as a single logical platform
- A node can be defined as an individual player in a distributed system
- The main challenge in distributed system design is **coordination between nodes and fault tolerance**



CAP Theorem

The theorem states that any distributed system cannot have **C**onsistency, **A**vailability, and **P**artition tolerance simultaneously:

- **Consistency** is a property that ensures that all nodes in a distributed system have a single latest copy of data
- **Availability** means that the system is up, accessible for use, and is accepting incoming requests and responding with data without any failures as and when required
- **Partition tolerance** ensures that if a group of nodes fails the distributed system still continues to operate correctly.

Consensus

- Consensus is a process of agreement between distrusting nodes on a final state of data.
- In order to achieve consensus different algorithms can be used.
- Easy between two nodes(for example in client-server systems)
- Difficult with multiple nodes (for example distributed systems)
- With multiple nodes is known as **distributed consensus.**

Consensus Mechanisms

- A consensus mechanism is a **set of steps** that are taken by all, or most, nodes in order to agree on a proposed state or value.
- For more than three decades this concept has been researched by computer scientists in the industry and Academia.
- Consensus mechanisms have recently come into the limelight and gained much popularity with the advent of bitcoin and blockchain.

Consensus Mechanisms- Requirements

- **Agreement**: All honest nodes decide on the same value.
- **Termination**: All honest nodes terminate execution of the consensus process and eventually reach a decision.
- **Validity**: The value agreed upon by all honest nodes must be the same as the initial value proposed by at least one honest node.
- **Fault tolerant**: The consensus algorithm should be able to run in the presence of faulty or malicious nodes (Byzantine nodes).
- **Integrity**: This is a requirement where by no node makes the decision more than once. The nodes make decisions only once in a single consensus cycle.

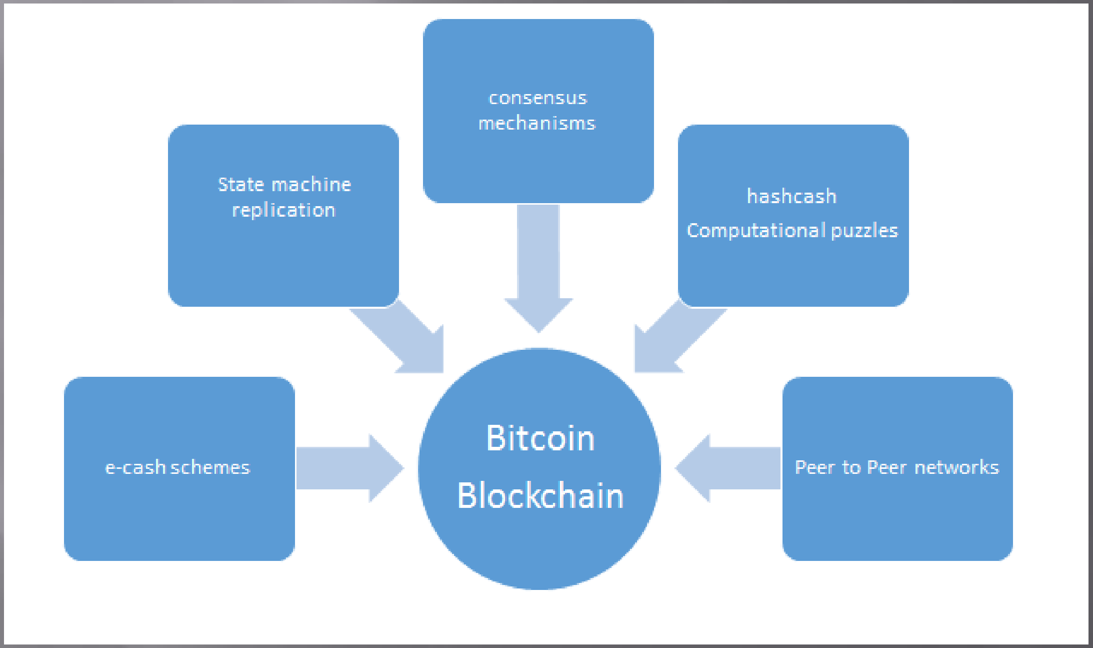
Consensus Mechanisms - Types

- **Byzantine fault tolerance-based**: With no compute intensive operations such as partial hash inversion, this method relies on a simple scheme of nodes that are publishing signed messages. Eventually, when a certain number of messages are received, then an agreement is reached.
- **Leader-based consensus mechanisms**: This type of mechanism requires nodes to compete for the *leader-election lottery* and the node that wins it proposes a final value.

Consensus Mechanisms - Background

- Many practical implementations have been proposed such as **PAXOS**, the most famous protocol introduced by Leslie Lamport in 1989. In Paxos nodes are assigned various roles such as Proposer, Acceptor, and Learner. Nodes or processes are named replicas and consensus is achieved in the presence of faulty nodes by agreement among a majority of nodes.
- Another alternative to Paxos is **RAFT**, which works by assigning any of three states, that is, Follower, Candidate, or Leader, to the nodes. A Leader is elected after a candidate node receives enough votes and all changes now have to go through the Leader, who commits the proposed changes once replication on the majority of follower nodes is completed.

Blockchain - History

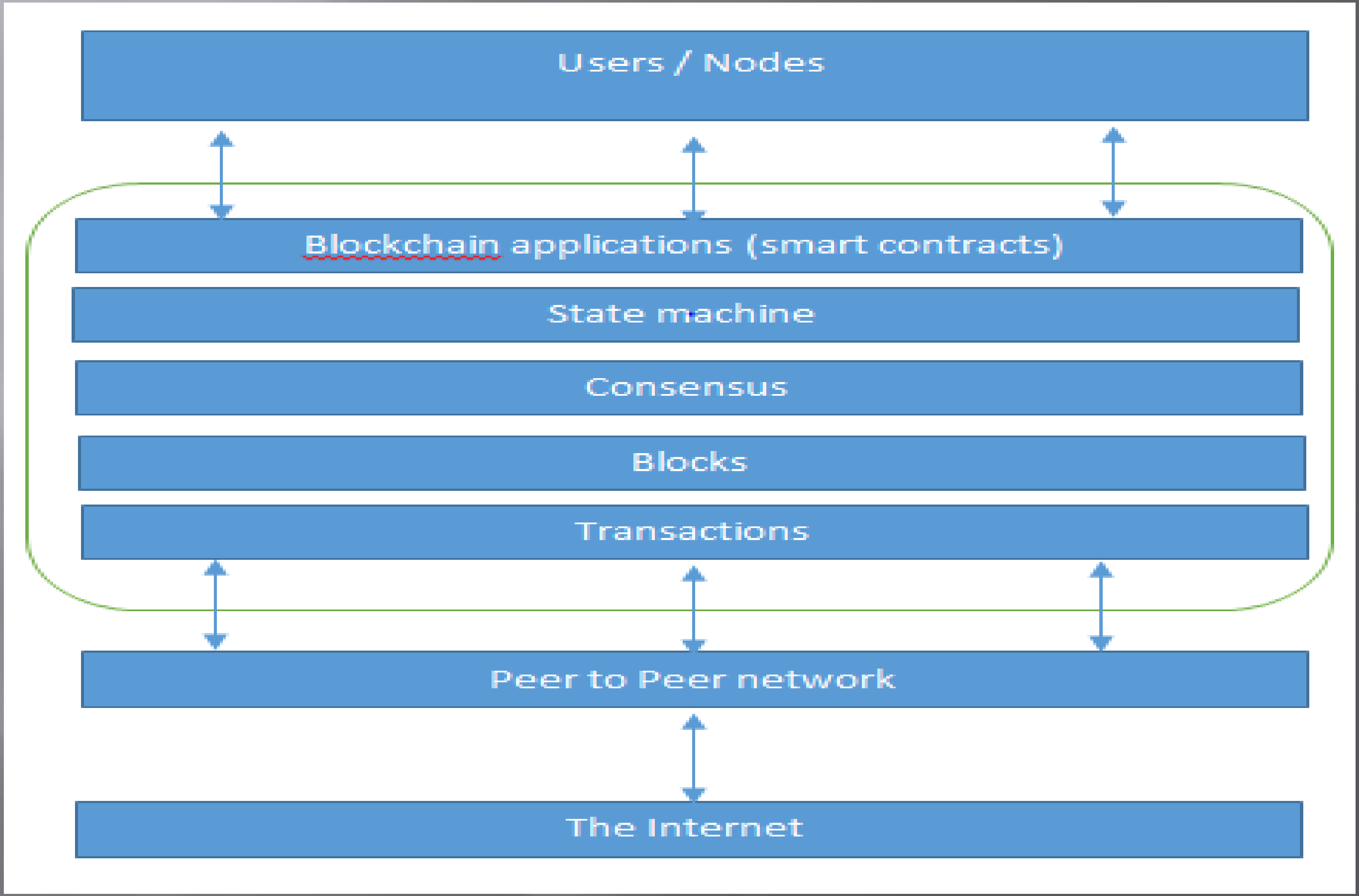


The various ideas that helped with the invention of bitcoin and blockchain

Blockchain - Introduction

Blockchain at its core is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.

Blockchain – A Network View



Blockchain - Technical Definitions

- Blockchain is a **decentralized consensus mechanism**. In a blockchain, all peers eventually come to an agreement regarding the state of a transaction.
- Blockchain is a **distributed shared ledger**. Blockchain can be considered a shared ledger of transactions. The transaction are ordered and grouped into blocks.
- Blockchain is a **data structure**; it is basically a linked list that uses hash pointers instead of normal pointers. Hash pointers are used to point to the previous block.

Blockchain - Generic elements

- Block
- Transactions
- Addresses
- State Machine

- Nodes
- P2P network
- VM
- Scripting Language
- Smart Contracts

Blockchain – Functions & Features

FUNCTIONS

- Distributed consensus
- Transaction verification
- Platforms for smart contracts
- Transferring value between peers
- Generating cryptocurrency

FEATURES

- Smart property
- Provider of security
- Immutability
- Uniqueness
- Smart contracts

Tiers of blockchain technology

- **Blockchain 1.0 –** Cryptocurrencies and Altcoins
- **Blockchain 2.0 -** Applications that are beyond currency, finance, and markets.
- **Blockchain 3.0 -** more general-purpose application sectors such as government, health, media, the arts, and justice.
- **Generation X (Blockchain X) -** This is a vision of blockchain singularity where one day we will have a public blockchain service available that anyone can use just like the Google search engine etc.

Blockchain - Types

1. Public blockchains
2. Private blockchains
3. Semi-private blockchains
4. Sidechains
5. Permissioned ledger
6. Distributed ledger
7. Shared ledger
8. Fully private and proprietary blockchains
9. Tokenized blockchains
10. Tokenless blockchains

Blockchain – Consensus Protocols

1. **Proof of Work(PoW)** : This type of consensus mechanism relies on proof that enough computational resources have been spent before proposing a value for acceptance by the network. Bitcoin
2. **Proof of Stake(PoS):** This algorithm works on the idea that a node or user has enough stake in the system; for example the user has invested enough in the system so that any malicious attempt would outweigh the benefits of performing an attack on the system. Peercoin

Blockchain – Consensus Protocols

3. **Delegated Proof of Stake (DPOS):** is an innovation over standard PoS whereby each node that has stake in the system can delegate the validation of a transaction to other nodes by voting. Bitshares
4. **Proof of Elapsed Time(PoET):** Introduced by Intel, it uses Trusted Execution Environment (TEE) to provide randomness and safety in the leader election process via a guaranteed **wait time.** Intel Sawtooth Lake blockchain project

Blockchain – Consensus Protocols

5. **Deposit-based consensus**: Nodes that wish to participate on the network have to put in a security deposit before they can propose a block.
6. **Proof of importance:** This not only relies on how much stake a user has in the system but it also monitors the usage and movement of tokens by the user to establish a level of trust and importance. Nemcoin.

Blockchain – Consensus Protocols

7. **Federated consensus or federated Byzantine consensus:** Used in the stellar consensus protocol, nodes in this protocol keep a group of publicly trusted peers and propagates only those transactions that have been validated by the majority of trusted nodes.
8. **Reputation-based mechanisms:** As the name suggests, a leader is elected on the basis of the reputation it has built over time on the network. This can be based on the voting from other members.
9. **Practical Byzantine Fault Tolerance(PBFT):** achieves state machine replication, which provides tolerance against Byzantine nodes.

CAP theorem and blockchain

- In blockchains consistency is sacrificed in favour of availability and partition tolerance.
- In this scenario, **Consistency** (**C**) on the blockchain is not achieved simultaneously with **Partition tolerance** (**P**) and **Availability** (**A**), but it is achieved over time.
- This is called *eventual consistency*, where

consistency is achieved as a result of validation from multiple nodes over time.

Blockchain – Benefits

- Decentralization
- Transparency and trust
- Immutability
- High availability
- Simplification of current paradigms
- Faster dealings
- Cost saving
- Highly secure

Blockchain – Limitations

- Scalability
- Adaptability
- Regulation
- Relatively immature technology
- Privacy