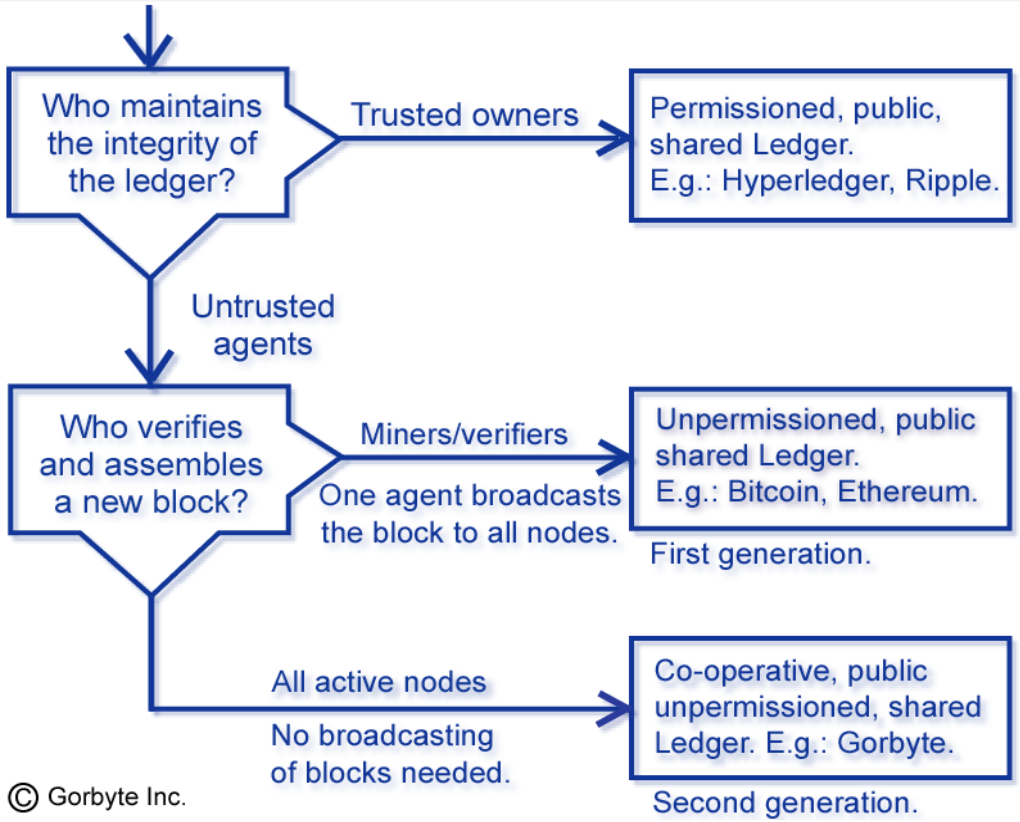
Evolution of Distributed Ledger Technology

The following diagram shows how, after the first attempts at decentralization in the 1990's, the Distributed Ledger Technology has progressed in the last few years, by using crypto-networks' blockchain technology and different consensus models:



Examples and classification

The following are examples of blockchain crypto-networks and how their consensus protocols can be categorized, referring to the two key questions in the previous diagram:

Who maintains the integrity of the ledger?

P: Permissioned: Trusted owners/agents:

- Ripple-based (a group of actors): **Tillit Ripple**, **Tembusu**, **Ripple Lab**.
- Decentralized group of trusted agents: **Hyperledger**, **Clearmatics**, **Eris**.
- Bitcoin-inspired blockchain, oracle-based: **MultiChain**, **Cryptocorp.**
- Flexible, Proof of Stake (PoS): **Tezos.**
- Sharding: **Disledger.**
- Trusted node-to-node paths: **Trustlines**.
- Federated:
  - (Cooperative foundation) **IOTA**,
  - (Flexible Trust, quorum) **Stellar**
  - (Private, Proof of Importance) **NEM**.

U: **Unpermissioned:** Untrusted agents (Practical BFT)**:**

Who verifies and assembles a new block?

L: **Leader-based:** One agent, among a "proven" set, verifies and broadcasts the new block (First gen. crypto-networks):

Proof of...

- *Work*: **Bitcoin, Ethereum** and similar: **Litecoin**, **Namecoin**, **Darkcoin**, **Dash**, **NimbleCoin**, and others.
- *Stake:* (random validators): **Tendermint**, **Algorand**, **Cardano**, **Peercoin**, **Blackcoin**, **NXT**, **Ethereum** (2018).
- *Elapsed Time*, in a trusted environment: **Intel**.
- *Activity* (PoW + PoS): No implementation.
- *Capacity* (Pay to play): **Burstcoin**.
- *Burn* (Pay to play): **Slimcoin**.
- *Importance* (rating accounts): **NEM**

C: **Cooperative: All active nodes** participate in block verification and equalization (Second gen. crypto-networks)**:**

Majority agreement, heuristic: **MARPLE** (by Gorbyte).

Note that many classic fault tolerant solutions (BFT, XFT, non-BFT), such as **Paxos**, **Raft**, etc., and Directed Acyclic Graph solutions, such as **IOTA Tangle,** and **Dagcoin**, are not designed for, or implemented on a blockchain.

MARPLE, by Gorbyte Inc.™

MARPLE, a new cooperative consensus protocol, is the key component of Gorbyte, a second generation crypto-network.

It distinguishes itself in the decentralization aspect of block assembly and equalization. Since all nodes are already broadcast every transaction, MARPLE reaches agreement by recursively equalizing blocks within Logical Environs. Gorbyte's security against DoS and majority attacks is also enhanced by its BRUD device architecture, allowing the detection and prevention of such attacks.

This combination allows for a higher throughput (from current crypto-networks 3-15 tps to 200-6000 tps), lower cost, a free service model, and scalability: every user device can participate as a full network node.

Properties of consensus (MARPLE):

- **Termination**: Every correct active node eventually decides.
- **Convergence**: A timeout can be set so that an arbitrary percentage of the correct active nodes terminate within the allotted block period.
- **Agreement**: No two correct active nodes decide different values.
- **Validity**: If the required majority threshold propose the same block B, then no value different from B can be decided.

Replication requirements (Gorbyte):

- Each node must commit to the same block within a certain time (synchronous, no forks).
- In most cases, transactions are broadcast only once. In the remaining cases only minimum exchanges are required, within a node environs.

MARPLE’s restrictions and assumptions:

- Randomization of sessions: Sessions established by a node at startup time connect to physically dispersed responding nodes (ASML protocol).
- Environs optimization: At node startup time, a minimum and maximum length of loops are allowed with network peers (FID protocol).
- Order restriction: Predefined rules for block normalization. This is essentially a restriction on the input values of the consensus process.
- Convergence timeout: Parametrically adjusted for an arbitrary minimum threshold of agreement. Late, disagreeable, or faulty nodes have to re-initialize.
- Synchrony assumptions: all nodes maintain the same timedate. The block collection period is predefined and synchronized.
- Cooperative assumption: Most nodes are cooperative, as they contribute their device’s resources to use free services. An attacker cannot replicate multiple nodes, because of the uniqueness imposed by the BRUD (virtual) device associated to each node.

MARPLE Attributes

MARPLE (Majority Agreement Recursive Protocol based on Logical Environs) is characterized by the following attributes:

- **Deterministic:** Consensus is irreversible – no forks are possible.
- **Synchronous period:** Nodes and block periods are synchronized, to increase the probability of similar blocks and to enforce time-outs.
- **Verification - Consensus independence:** Transaction processing and verification are independent from the consensus process and block composition.
- **Decentralized:** There is no master node, no set of miners, verifiers or generals, but each node participates in the consensus.
- **Heuristic:** Each node cooperates with a random set of peer nodes.
- **Cooperative:** Consensus is achieved by majority agreement, not by a set of competing agents (miners or verifiers).
- **Unpermissioned:** Nodes do not need to be given special permissions by an authority.
- **High throughput:** Most transactions are broadcast only once. Blocks are never broadcast. Most protocol messages are within node's environs, and happen in parallel.

Reference List of Networks Using Original Consensus Protocols

Abstract (Azyzzyva, Aliph, R-Aliph, ZLight)
https://infoscience.epfl.ch/record/208030/files/The_next_700bft_prot_a12-aublin.pdf

ACHAIN
https://www.achain.com/Achain_tech_white_paper_translate.pdf

ALGORAND
https://arxiv.org/pdf/1607.01341.pdf

BitShares
https://bitshares.org/technology/delegated-proof-of-stake-consensus/

CARDANO
https://www.cardanohub.org/en/home/

CREDITS
https://credits.com/

DagCoin
https://bitslog.wordpress.com/2015/09/11/dagcoin/

DisLedger
https://www.disledger.com/DisLedger_TokenLaunch.pdf

ELASTICO
https://www.comp.nus.edu.sg/~loiluu/papers/elastico.pdf

IOTA Tangle
https://iota.org/IOTA_Whitepaper.pdf

Mastercrypt
http://drops.dagstuhl.de/opus/volltexte/2017/7093/pdf/LIPIcs-OPODIS-2016-24.pdf

MultiChain
http://www.the-blockchain.com/docs/Multichain%20Whitepaper.pdf

NEM
https://nem.io/

NXT
http://nxtcrypto.org/nxt-technology/more-nxt-proof-stake-forging

Paxos
https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/The-Part-Time-Parliament.pdf

Raft
https://www.usenix.org/system/files/conference/atc14/atc14-paper-ongaro.pdf

Sieve
http://drops.dagstuhl.de/opus/volltexte/2017/7093/pdf/LIPIcs-OPODIS-2016-24.pdf

Stellar
https://www.stellar.org/papers/stellar-consensus-protocol.pdf

Tendermint:
https://tendermint.com/static/docs/tendermint.pdf

Zlight
https://infoscience.epfl.ch/record/208030/files/The_next_700bft_prot_a12-aublin.pdf

Zyzzyva
http://www.cs.utexas.edu/users/dahlin/papers/Zyzzyva-CACM.pdf