

◆ BIG DATA

◆ DISTRIBUTED REGISTRIES

◆ ECOSYSTEM

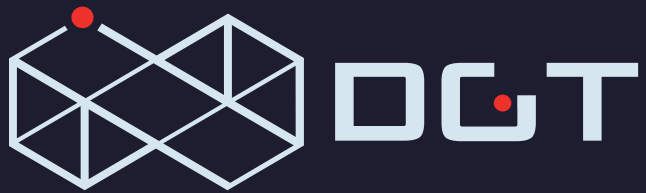


F-BFT CONSENSUS

Integrating Distributed Data Sources

DETAILED INFORMATION

PLATFORM



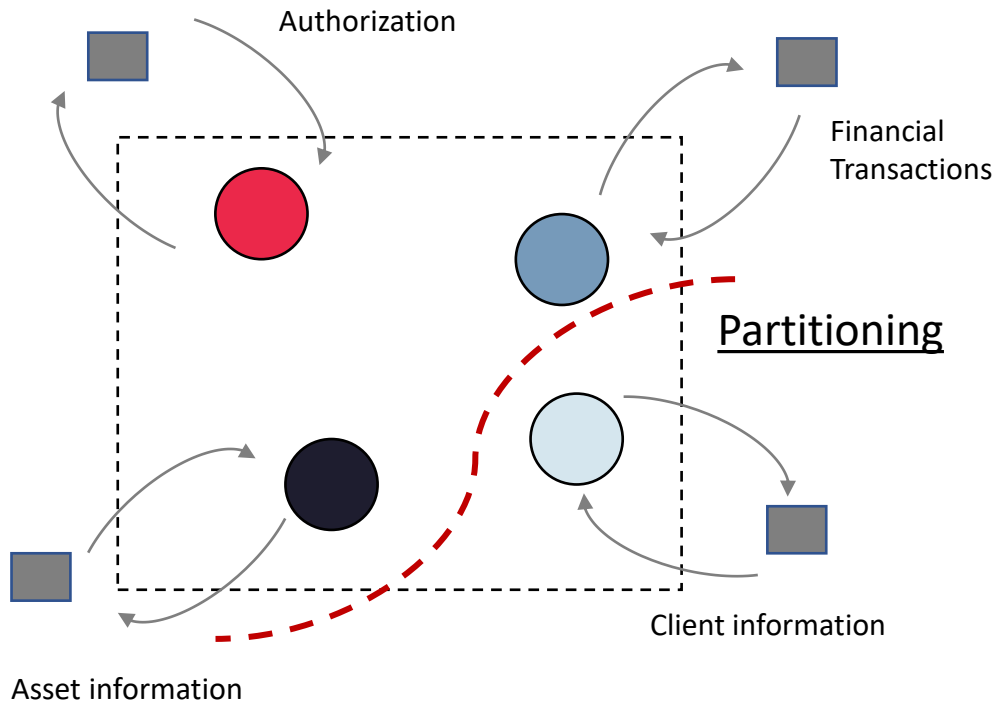
A Multifunctional Data Platform for creating a unified information space between distributed data sources

In systems with many participants, a consensus is generally understood as a mechanism for ensuring a commonly validated set of data that is uniform for all participants in the information exchange

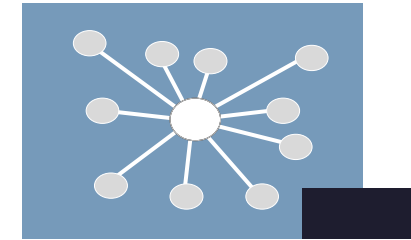
The F-BFT Consensus Algorithm forms the basis for integrating distributed data

DECENTRALIZATION AND DISTRIBUTION

Participants that are looking for coordination are united into a network, which can have different topologies – including centralized, decentralized, and distributed. The distribution and decentralization are not absolute values and may vary from solution to solution



Networks can break up into fragments (partitioning), nodes may be inaccessible due to their SLA³ – all of these influence the totality, integrity, and availability of data in the network.



Centralized Network



Decentralized Network



Distributed Network

Depending on the network's parameters, its characteristics influence data:

- Throughput – how many transactions can be done in a period of time (TPS)⁴;
- Latency – how much time each transaction takes;

The data consensus mechanism depends on the level of decentralization and distribution and affects TPS and latency

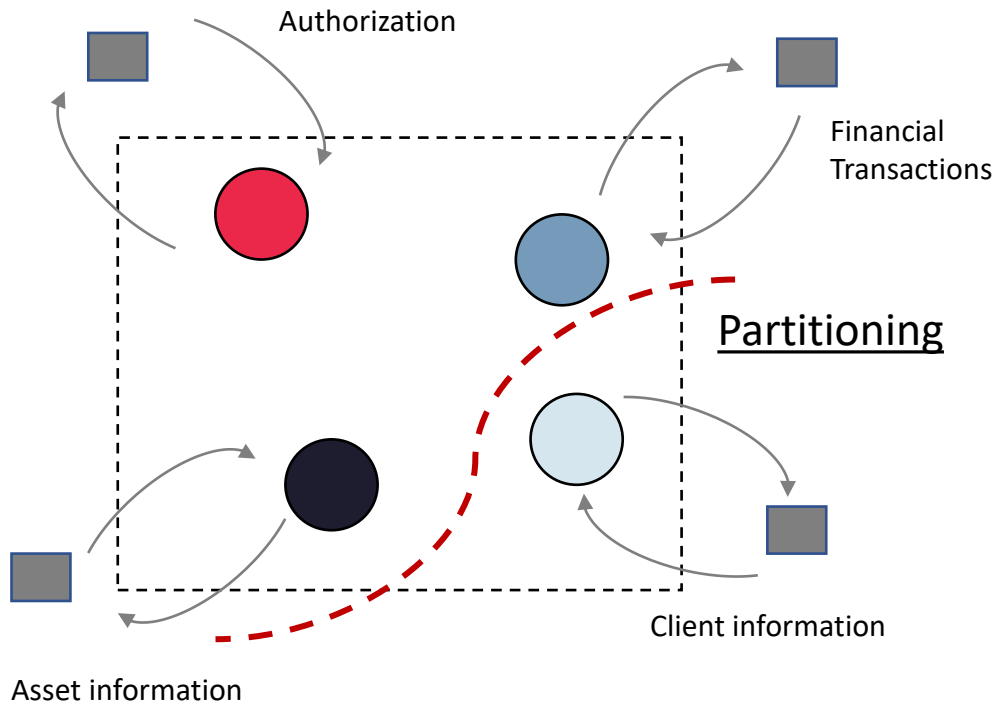
3

³) SLA (Service Level Agreement) – the level of power and performance of distinct nodes

⁴) TPS – transaction per seconds, the performance of a computing system in relation to the number of transactions processed per second

The data consensus mechanism depends on the level of decentralization and distribution and affects TPS and latency

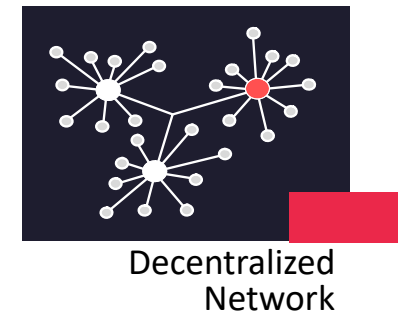
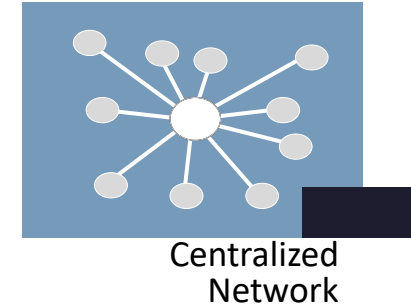
Participants that are looking for coordination are united into a network, which can have different topologies – including centralized, decentralized, and distributed. The distribution and decentralization are not absolute values and may vary from solution to solution



Networks can break up into fragments (partitioning), nodes may be inaccessible due to their SLA³ – all of these influence the totality, integrity, and availability of data in the network.

Depending on the network's parameters, its characteristics influence data:

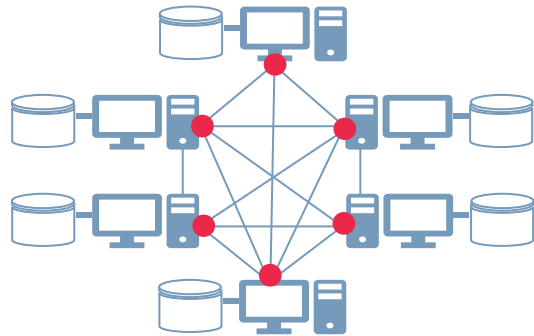
- Throughput – how many transactions can be done in a period of time (TPS)⁴;
- Latency – how much time each transaction takes;



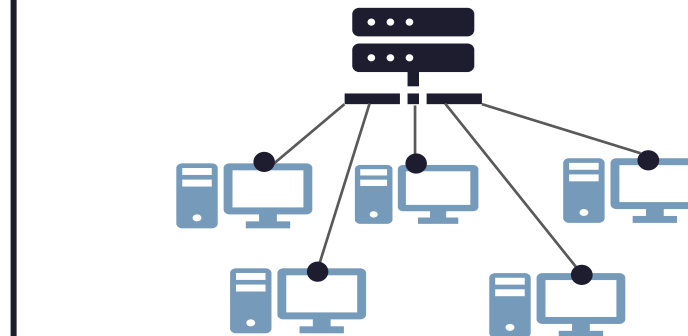
³ SLA (Service Level Agreement) – the level of power and performance of distinct nodes

⁴ TPS – transaction per seconds, the performance of a computing system in relation to the number of transactions processed per second

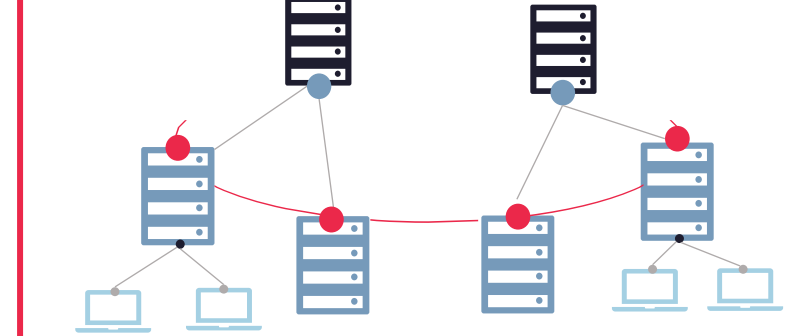
The consensus mechanism depends on the network topology



(single rank) Peer-to-peer networks



(multi-rank) Client-server networks



(multi-rank) Hybrid networks

Client-server networks

- ✓ **control over network composition** — strict control of connected networks (strong authentication);
- ✓ **single point of data collection** — with the ability to control data at a single point;
- ☹ **powerful server required** — no horizontal scalability;
- ☹ **individual nodes cannot operate independently** — uniformity is required;

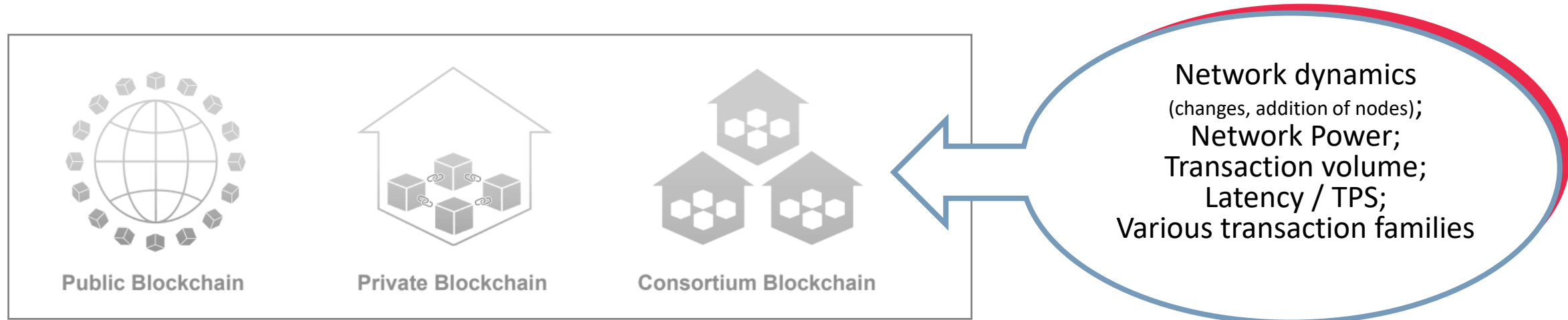
Hybrid networks may compensate for the flaws of client-server and P2P networks through its flexible policy

P2P networks

- ✓ **scalability** — there is no bottlenecking at any point of the network, since the information exchange can occur between end nodes;
- ✓ **durability** — network operability is maintained when almost any number of nodes are disconnected from the network;
- ✓ **privacy** — user data may be stored locally; while calculations are performed directly on personal computers, without involving a trusted third party;
- ☹ **vulnerability** — to “byzantine attacks”, particularly data substitution and traffic manipulation;
- ☹ **data quality control** — requires special verifications

⁵⁾ SCALABILITY – the ability of a system to manage increasing loads. Vertical scaling: increase in performance through increasing the capacity of individual components. Horizontal scaling: parallel processing and increasing processing through the network’s structure.

The order of joining the network determines the degree of trust in the nodes and the ability to accept transactions from them to be written into the joint general ledger



- Public Blockchains — fully open, where every node can participate in the vote (data reconciliation), where transactions are not controlled and are carried out freely;
- Private Blockchains – all transactions are tracked and controlled by a centralized body;
- Consortium Blockchains – voting is controlled by select nodes;

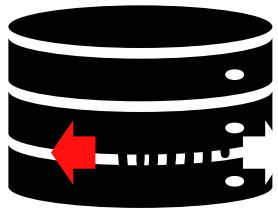
The estimated number of nodes to be connected, their lifetimes, and the stability of the entire network have a significant impact on the network architecture.

The data consensus mechanism is largely determined by the order of reading and writing data messages (transactions); different consensus use different data writing algorithms

The organization of the data storage system, data synchronization, the procedure for nodes to write data into the common registry – all impose restrictions on the data architecture and the general approach to

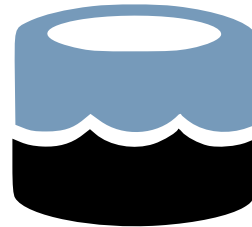
integration

Distributed Ledger Technologies (distributed ledger technologies); including blockchain solutions



Relational databases

The distribution of data sources is resolved through replication and ETL⁶ downloads



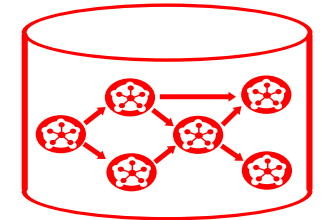
Data lakes
(NoSQL databases)

Rejection of the absolutism of ACID⁷ principles, transition to base architecture



Blockchain

Data storage in blocks that have imposed restrictions. In practice, block storage is a linear collected list.=



DAG – based solutions

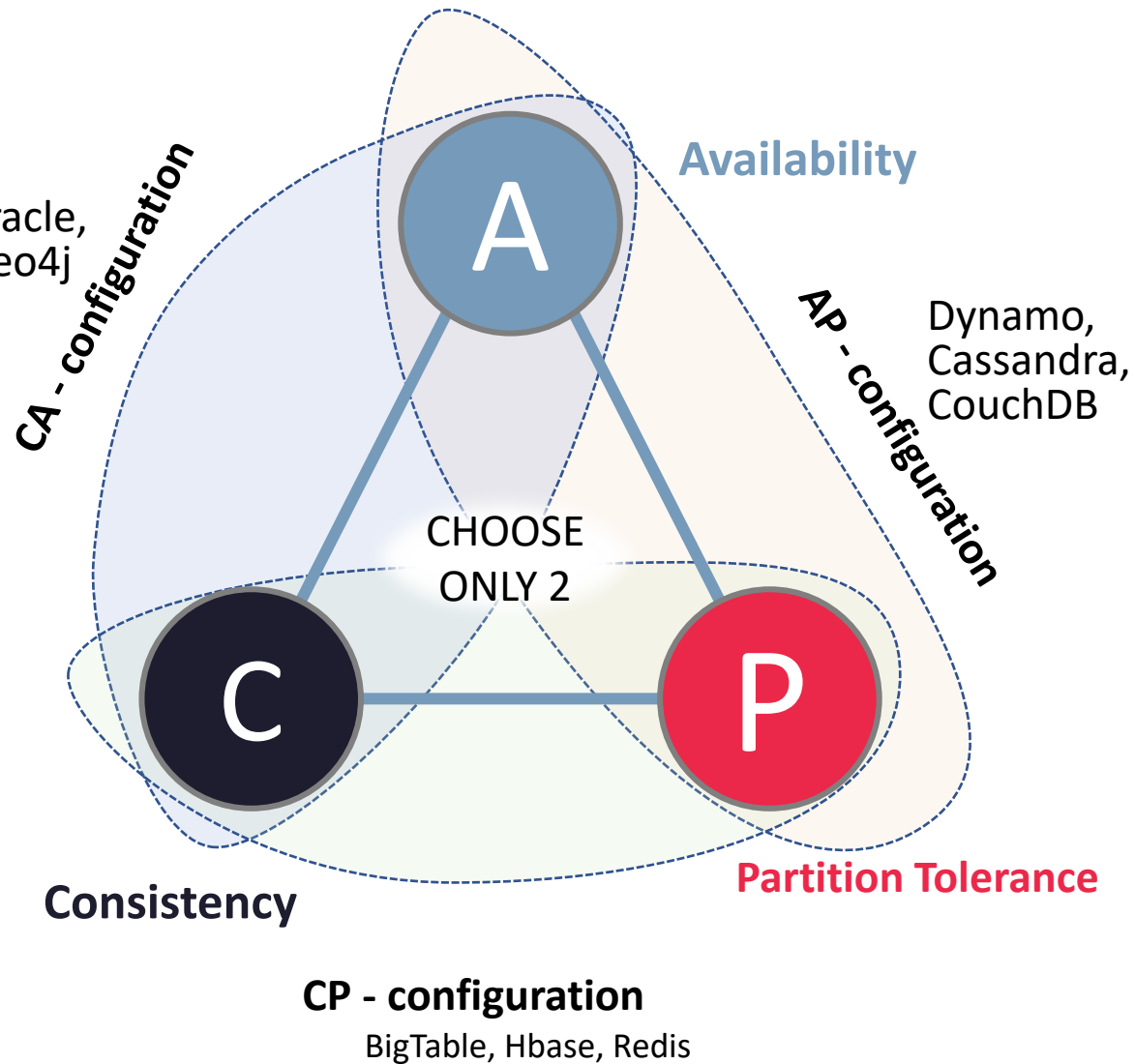
Storage in graph databases (DAG), where connections between data is stored in addition to data itself; branching is possible

⁶) ETL – Extract, Transform, Load: the process of moving data into a central repository;

⁷) ACID – requirements for a transaction system (Atomicity, Consistency, Isolation, Durability)

⁷) BASE – the storage architecture common for blockchains and big data; which provides basic availability, soft stage, and eventual consistency;

⁸) DAG – Directed Acyclic Graph – this structure is often used for computational tasks due to its topological sorting capability in finite time;



The CAP Theorem (Brewer's Theorem) – is a heuristic statement that for any implementation of distributed computing, only two of the following three properties may be attained: data consistency (lack of contradictions at any one point of time), availability (any request to the system ends with a correct response); and partition tolerance (tolerance to being divided into parts).

The PACELC Theorem — is an expansion of the CAP Theorem: in case a distributed computing system network is partitioned (P), you must choose between availability (A) and consistency (C), but in any case, even if the system works fine without division, you must choose between latency (L) and consistency (C).

The consensus mechanism can be interpreted as resistance to certain attack vectors (“double spending”, Sybil attack, 51% attack, Byzantine attacks)

All information systems are vulnerable. Distributed systems are vulnerable to the so-called Byzantine Fault (based on a classic Byzantine Generals problem). This reflects the features of distributed systems in failures occurring when the status of system component (node) is unknown, which could be functioning incorrectly or be inaccessible

THE BYZANTINE GENERALS PROBLEM

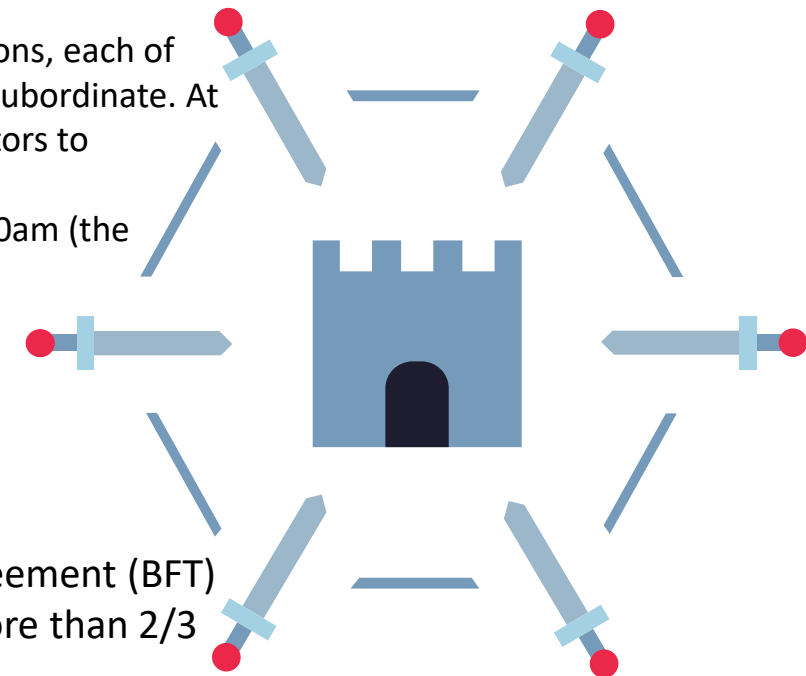
Byzantium. It is the night before a great battle with a mortal enemy. The Byzantine army is composed of n legions, each of which is commanded by its own general. The army also has a commander-in-chief, to whom the generals are subordinate. At the same time, the empire is in decline and any of the generals and even the commander-in-chief may be traitors to Byzantium, interested in its defeat.

At night, each of the generals receives an order from the leader providing a version of actions to be taken at 10am (the time is the same and known to everyone), in particular whether to “attack” the enemy or “retreat”.

Possible outcomes of the battle:

- If all loyal generals attack – Byzantium will defeat the enemy (good result).
- If all loyal general retreat – Byzantium will keep its army (intermediary result).
- If some loyal generals attack, while others retreat – the enemy will defeat the entire Byzantine army (bad result).

According to Lambert’s theorem, in any system with m incorrect nodes (“disloyal general”), agreement (BFT) can be achieved only if there are $2m + 1$ correct processors (“loyal generals”), that is, strictly more than $2/3$ of the total number of processors (provided that messages are subject to change in transit).



9

In the general case, with a variable number of nodes, the theoretic BFT problem is not solvable. But for systems with constraints, there are P-BFT, PAXOS, and RAFT algorithms.

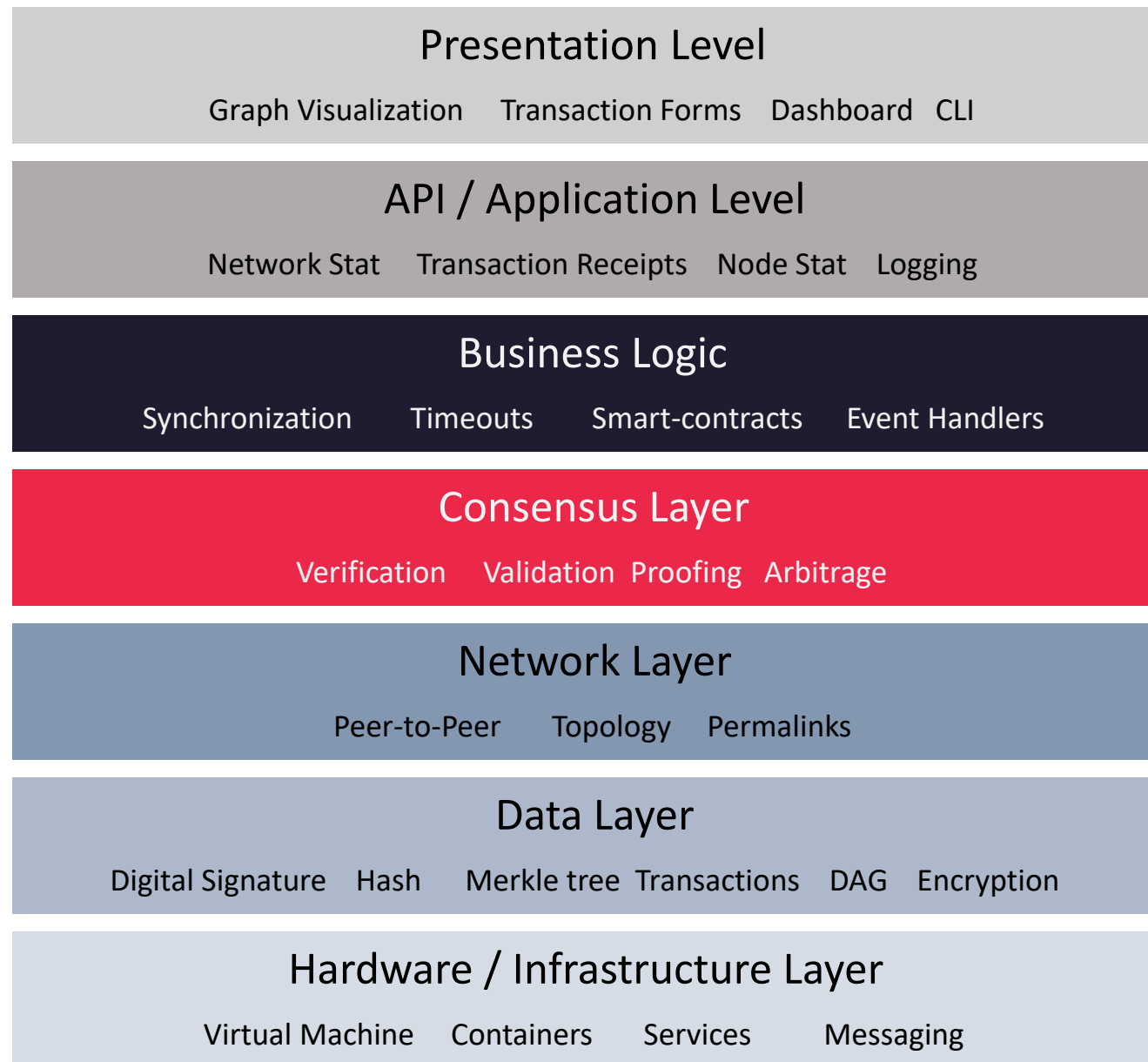
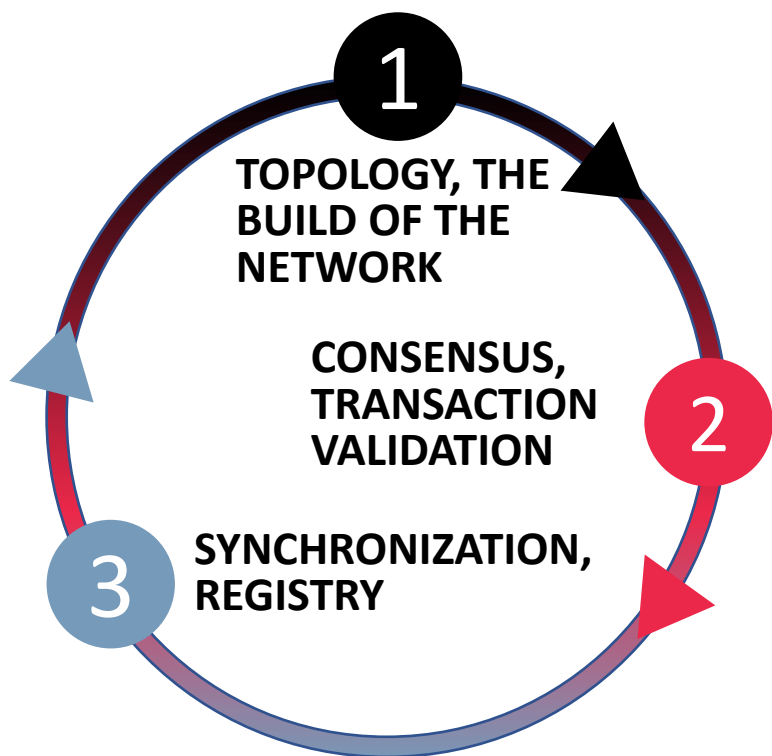
There is a large number of different systems for processing distributed information sources. Their classification and selection for the implementation of practical scenarios is difficult due to the following circumstances:

- There is confusion between consensus mechanisms (algorithms) and platforms. There are many more platforms, while some allow for the use of varying consensus;
- High levels of hype around cryptocurrencies attracted a large number of unprofessional teams that released clones or derivative solutions;
- The solution market has not stabilized, in particular, there has been no separation between platform and protocol developers, between network operators and application developers ⁹;
- There is a negative influence of pseudo-decentralized solutions, such as crypto-exchanges, Hyperledger Fabric and etc.;
- The complexity of the choice itself in terms of taking into account the multidimensional criteria, including the openness of permissions, workloads, and requirements for the information storage system



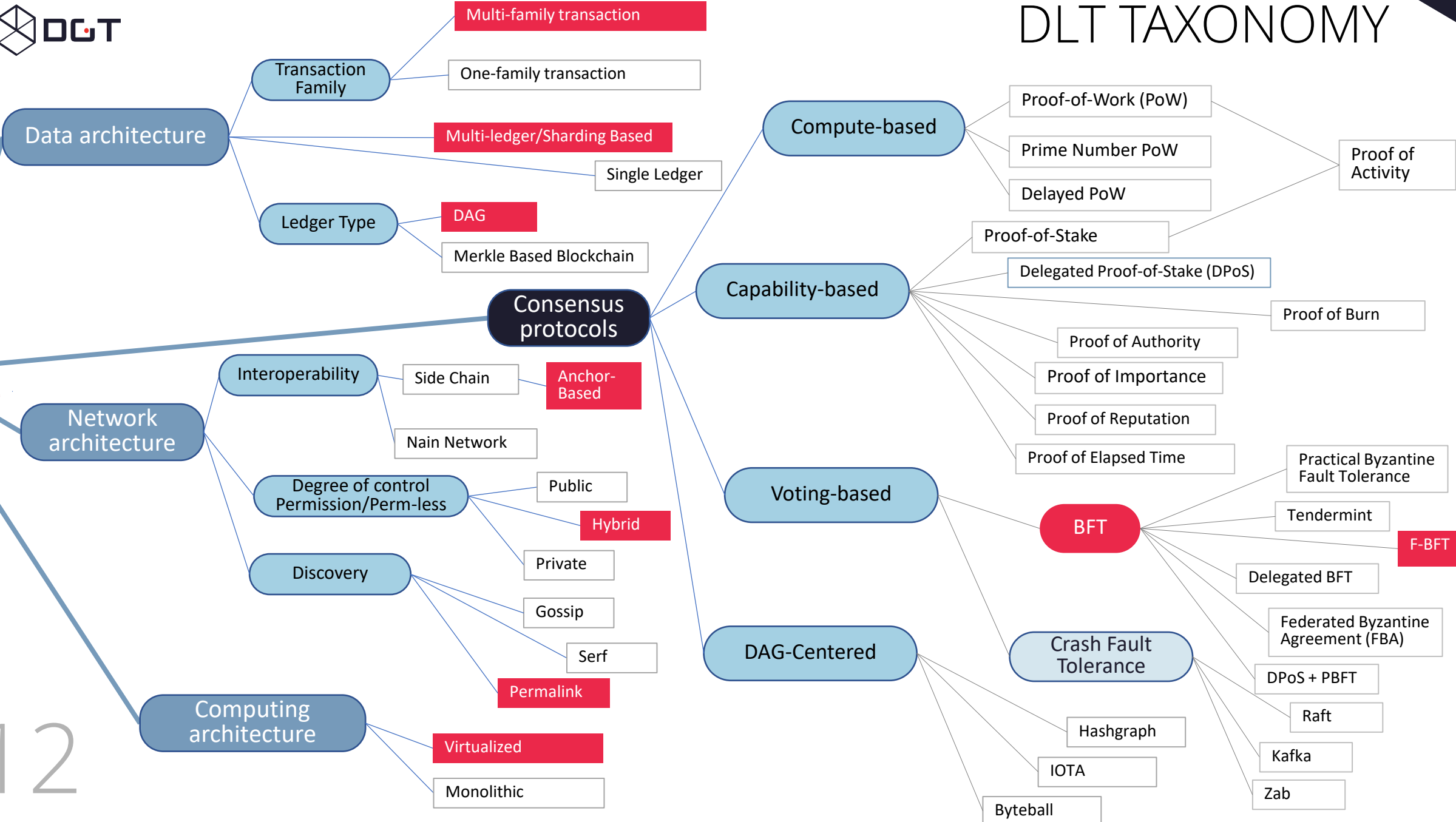
The reference architecture addresses the platform's functionality with a single systematic approach.

From a computational point of view, any distributed platform solves three fundamental problems of distributed ledgers:



DLT

12



	PROOF-OF-WORK	BFT-BASED PROTOCOLS	DGT (AUGMENTING BFT ¹¹)
NODE IDENTIFICATION	Fully open, public network	Node ID's managed for private networks	Hybrid network based on a flexible KYC mechanism
THROUGHPUT	! Limited: due to risk of forks	Great: (ten thousand TPS)	Great: as for all BFT
LATENCY	! High: each block to be approved by many	Very low: defined by network delays	Very low: federative structure allows for better organization of communication within (functionally) close groups
POWER CONSUMPTION	! High: useless computing work	Great: does not require high computing power	Great: same as BFT
SCALABILITY	Many participants	! Limited: small # of nodes; closeness to centralized tech	High: horizontal & vertical scalability due to federal structure and DAG ledger
CORRECTION OF SELECTION PROCESSES	No	Yes	Yes

¹⁰⁾ According to SLA (Service Level Agreement) – the level of power and performance of individual nodes

¹¹⁾ F-BFT is ideologically based on BFT, but contains a number of improvements, such as the use of DAG, federative structure, arbitrage and so forth

DGT DGT PLATFORM

The main motivation for creating a platform is to implement a hybrid system of working with distributed information sources for the implementation of the three most complex integration methods:

- Marketplaces (relatively independent participants);
- Ecosystems;
- Holding structures (vertical integration).

At first, we considered systems based on Ethereum and Hyperledger Fabric, as well as Hedera Hashgraph.

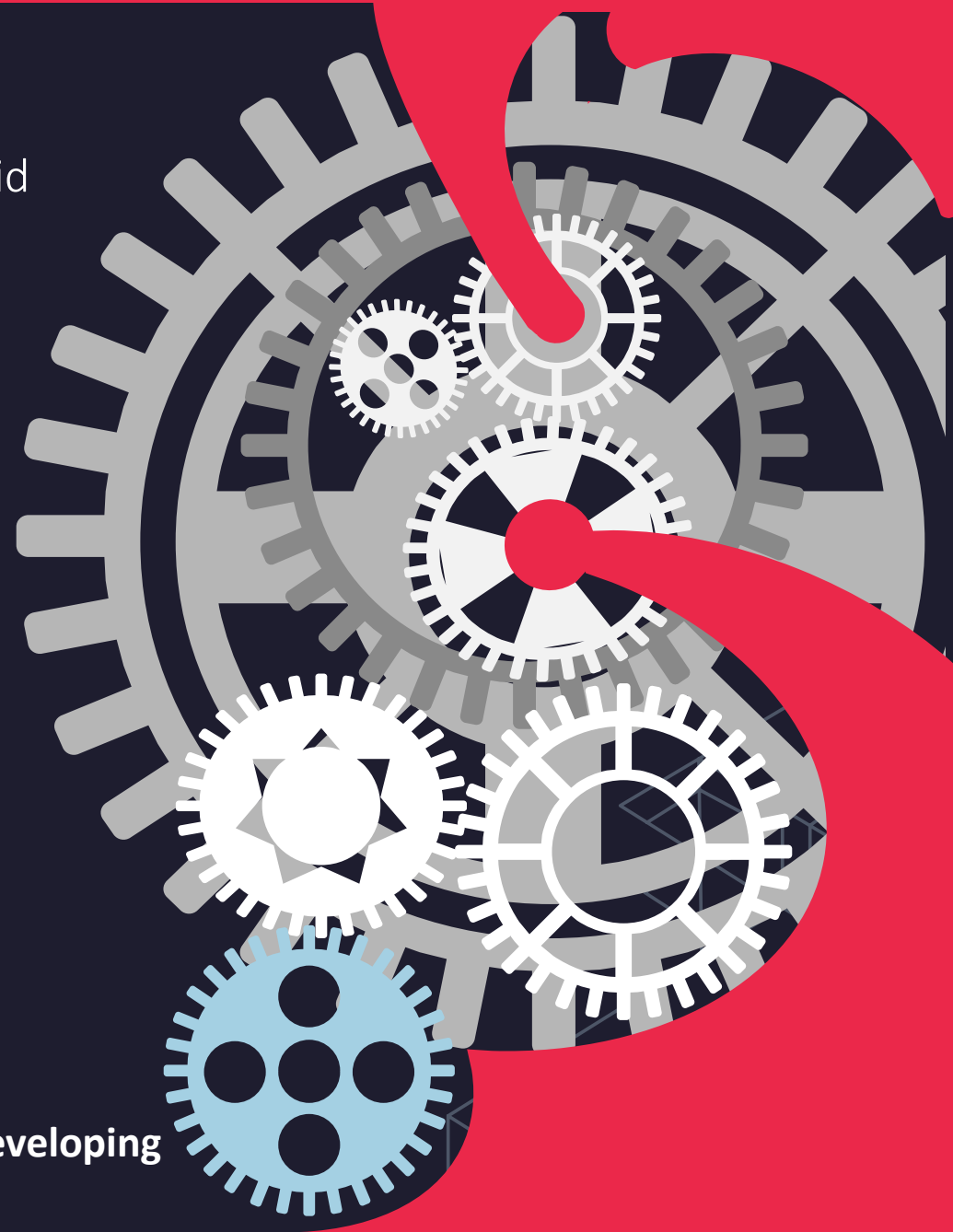
Reasons we began development of our own consensus:

- The lack of any necessary degree of decentralization and the closed nature of the Hyperledger Fabric network;
- The need to be tied to a mining mechanism and the low performance speed for PoW-based platforms;
- The necessity to establish a multi-transactional system;

14

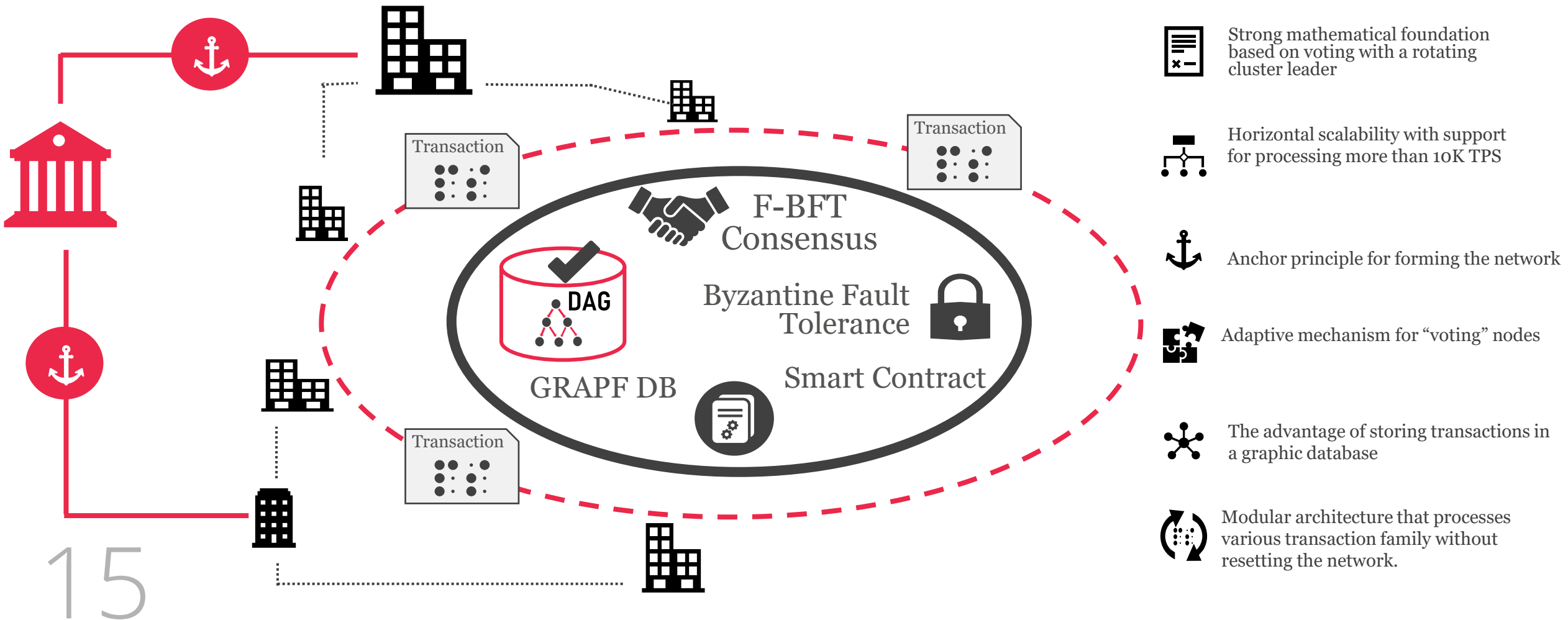


**In the end, we made a decision to begin developing
as a fork of Intel Sawtooth**

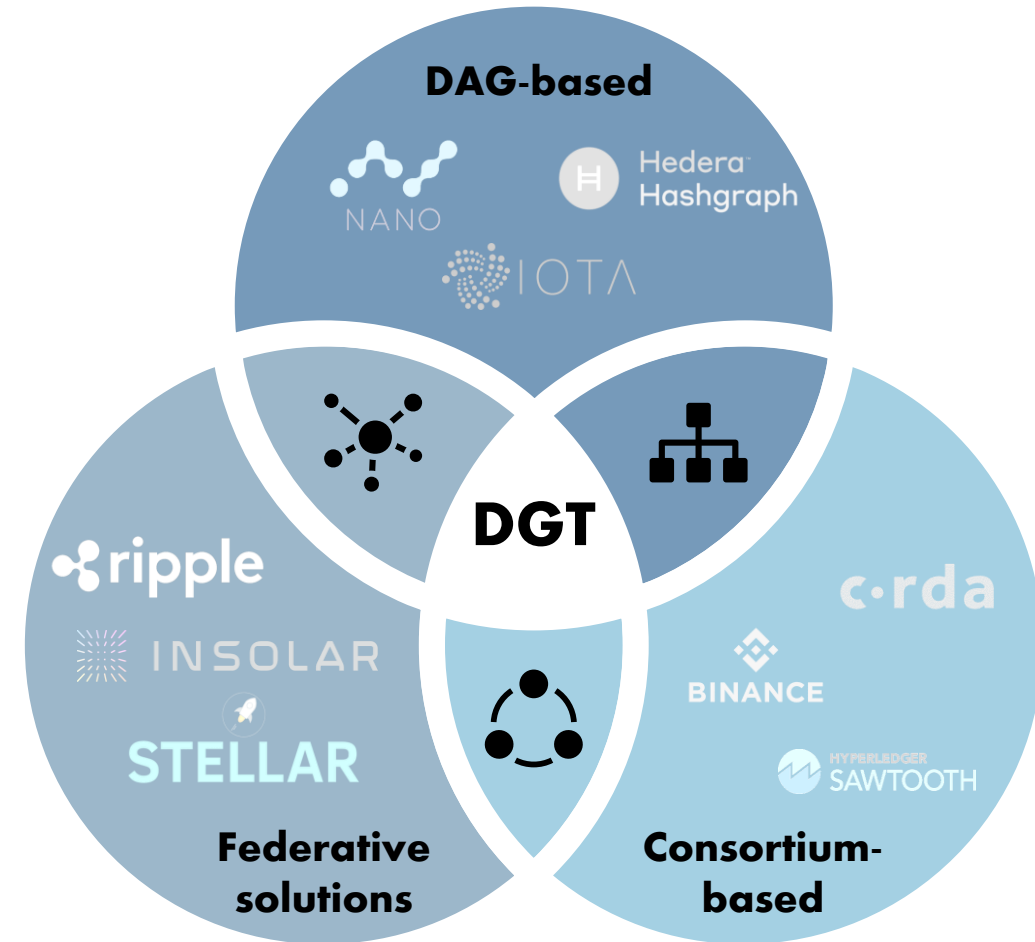


The heart of the DGT platform is the proven F-BFT consensus

The federated consensus mechanism works in a hierarchal environment, placing transactions into graph nodes...









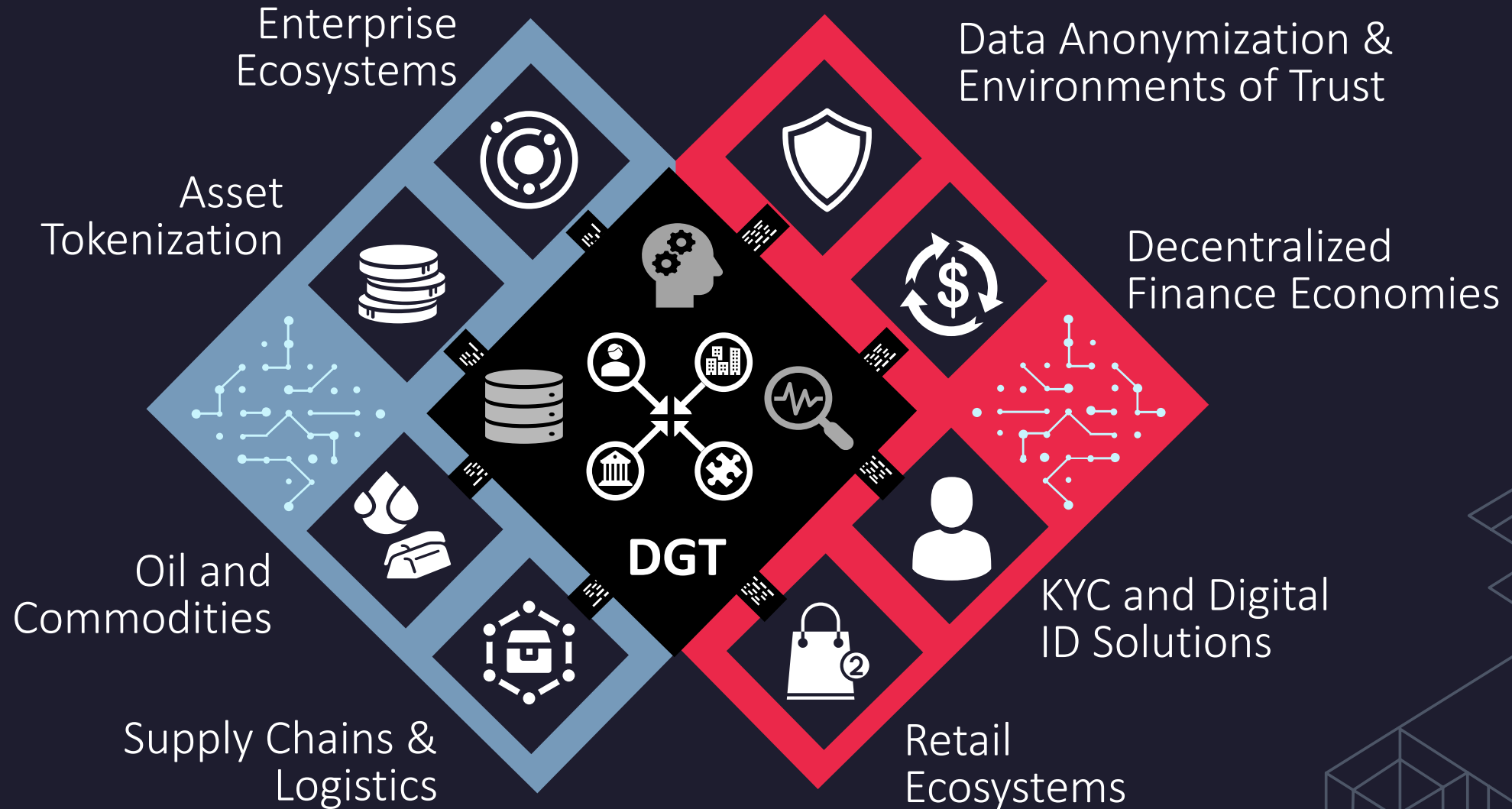
- **The storage system is based on DAG**, like IOTA, Hedera Hashgraph, Orumesh, DagCoin, Byteball, Nano. The DGT approach differs from these systems in that it allows for voting in a federated network structure with configurable topology;
- **The federative approach** to voting is actively used by such solutions as Ripple, Stellar. DGT brings transposes this ideology onto a horizontally scalable DAG and provides dynamic topology through rotating cluster leaders. This ensures network stability;
- **The consortium-based consensus** systems allows for flexibility, without sacrificing speed and interoperability. For example, Hyperledger Fabric targets private peer-to-peer networks and requires the formation of special sidechains, while ICON's solution uses a special Loopchain Fault Tolerance mechanism to interact with other networks. Unlike such solutions, DGT implements a dynamic topology on top of DAG, allowing for highly asynchronous network operation.





COMPETITIVE ALTERNATIVES

	Purpose	Network Organization	Consensus	Data Storage	Tokenization	Smart Contracts	Encryption
 DGT	Integration of enterprise data in real time; business ecosystems	Federative Consortium-based	F-BFT	DAG	Yes	Yes	Asymmetric, ECDSA curve secp256k1
 Ethereum	Distributed calculations, crypto, smart contracts	Single level Public	PoW	Blocks	Yes	Yes	ECDSA
 Stellar	Payment Network	Single level Public	FBA	Blocks	No	Yes	Asymmetric, ED25519
 EOS	Distributed calculations, crypto	Single level Public	dPOS	Blocks	Yes	Yes	ECDSA secp256k1
 IOTA	Micropayments, IOT, crypto	Single level Public	FPC (MCMC)	DAG	No	Yes	Kerl
 HYPERLEDGER	Data exchange in a corporate environment	Single level Private	P-BFT	Blocks	No	Yes	PKCS11,, pluggable



THANK YOU

info@dgt.world



medium.com/@dgtworld



www.dgt.world

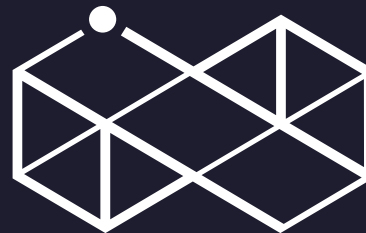
WWW



twitter.com/dgtnetwork



CONNECT TO



DGT

