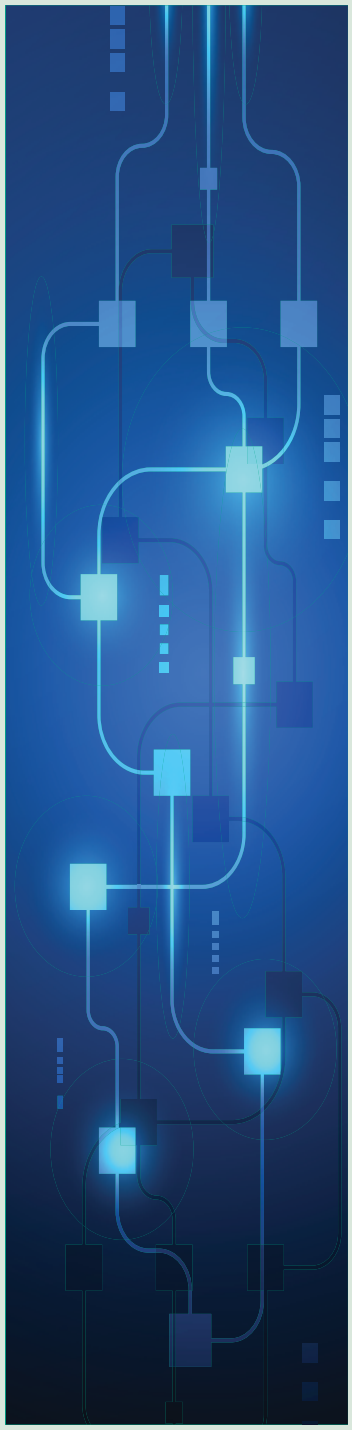
WHITE PAPER



EVOLUTION OF DISTRIBUTED LEDGER TECHNOLOGY PLATFORMS

Infosys®
Navigate your next

Distributed Ledger Technology or DLT, is a distributed system of records which are recorded across multiple sites that are not controlled or authorized by any single entity

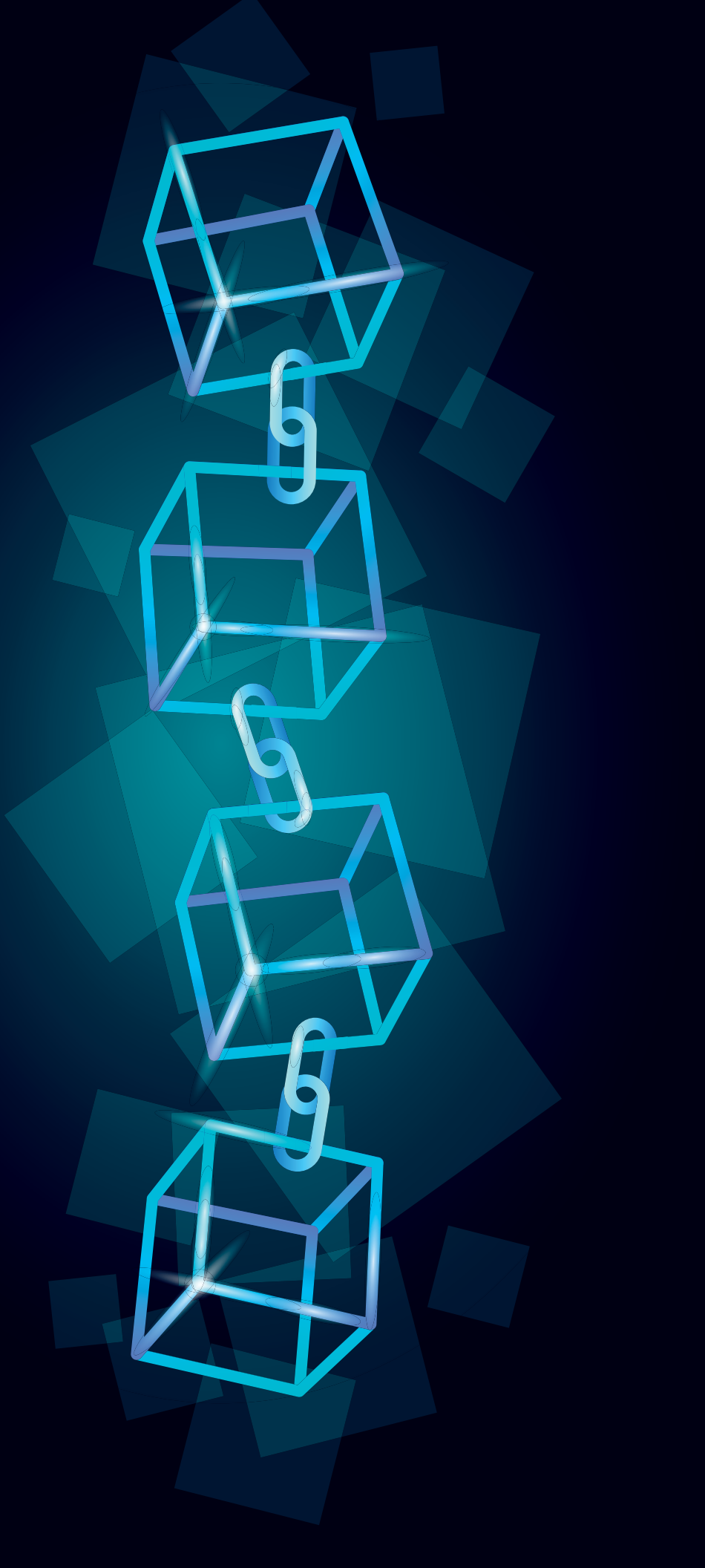
The term "Distributed" could have multiple inferences – conventionally, of a ledger physically split or replicated across multiple repositories, with no intermediary driving complete control over it.

DLT enables secure processing and transparency in a group of parties that lack trust, and that need to arrive at an agreement on adding a transaction, and the sequence in which it is added. Trust is mandatory to a DLT and is brought about by an automated consensus algorithm.

There are a variety of DLTs, each with its own unique characteristics. While the basic parameters of DLT are retained, each design caters to specific requirements of a usecase, and may not be appropriate for many other usecases.

The key parameters which constitute and differentiate a DLT are:

- **Decentralization** – no single entity controls or dictates acceptance and sequencing of transactions, however there needs to be a degree of consensus among stakeholders. Consensus could be arrived at using a variety of algorithms, the choice of which is often governed by usecase imperatives. Therefore, a Proof of Work consensus based DLT would never fit a usecase that witnesses high transaction volumes
- **Performance** – The ability to match and improve throughput (transactions per second) for a usecase from its as-is current state to its DLT based state. While certain DLTs and Blockchains witnessed slow adoption at the outset due to performance issues, others transformed themselves to increase throughput using a variety of levers – altering consensus mechanism, sharing data with participants only on a need to know basis and reducing system stress, optimizing data stored on the chain
- **Security** – The essence of security and confidentiality of transactions on blockchain is the common factor across all DLTs. The data that is cryptographically hashed, varies depending on the usecase imperatives. Multi factor authentication in different combinations provides added security



Then there is Blockchain

Blockchain is a type of DLT, perhaps the first fully serviceable one as the platform for cryptocurrency. With increasing hype, the term Blockchain is often used interchangeably with DLT. A key aspect that sets Blockchain apart from the other DLTs is how transactions are stored. In Blockchain, cryptographic hash of transactions are bundled in blocks, which are linked together to form a chain – hence the name.

Blockchain technology has evolved at a rapid pace since it was acknowledged as a major disruptor. Technology enthusiasts across the spectrum including Consortia, Fintechs, and Stakeholders that are most impacted by Blockchain, have been actively investing in development of the technology to enhance its adoption and proliferation.

DAG based DLTs

As a consequence of these initiatives, the crypto landscape continues to evolve, with a plethora of DLTs, that are not Blockchains , namely – IOTA, HASHGRAPH, NANO, PEAQ, CONSTELLATION, FANTOM. These are mostly based on the Directed Acyclic Graph pattern. The DAG based DLTs are intended to retain the strengths of blockchain, while they endeavor to improve its weaknesses. While all DLTs offer transparency and security, the DAG based DLTs endeavor to overcome the intrinsic scalability challenge of Blockchains. A DAG based ledger is such that the throughput grows proportionately to the depth or size of the ledger. Therefore, the larger the network the faster it is.

Enclosed below is a brief overview of a few of the most distinct of DLTs that are not Blockchains.

R3 CORDA

Corda was visualized as a Distributed ledger for recording and processing Financial transactions with the goal to enhance scalability, while maintaining data consistency. Corda maintains ledgers in a Peer-to-Peer model, and does not offer a single or common ledger. Each node stores data corresponding to the transactions it is party to. Hence, there is no single node that is aware of the ledger in its entirety – this in essence also adds a layer of security. It supports Smart Contracts as agreements that are both automatable and enforceable.

Corda implementation does not lock into any specific Consensus model, leaving the selection to be governed by the usecase. It eliminates the need to arrive at a consensus across all parties in the network. Instead the actors participating in a transaction are the ones to store the transactions.

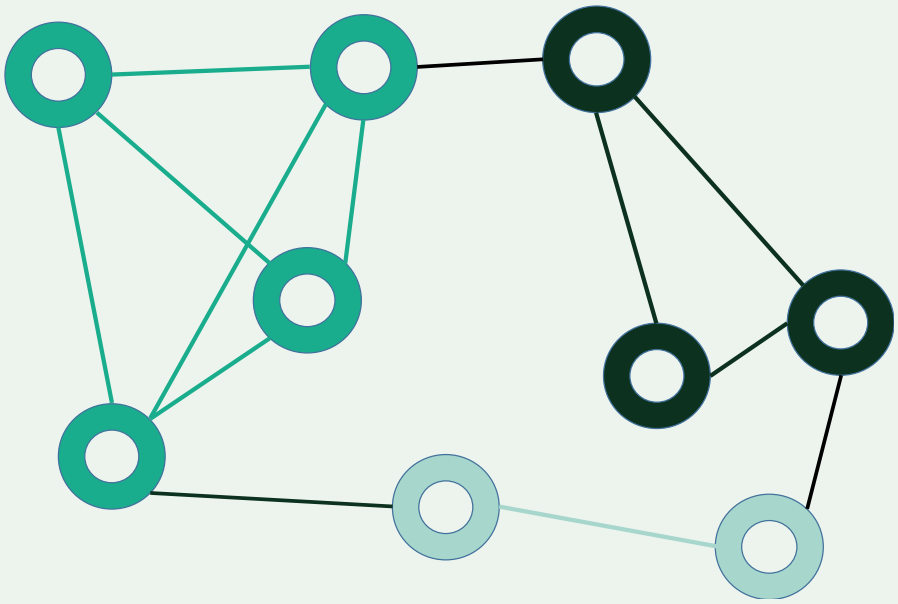
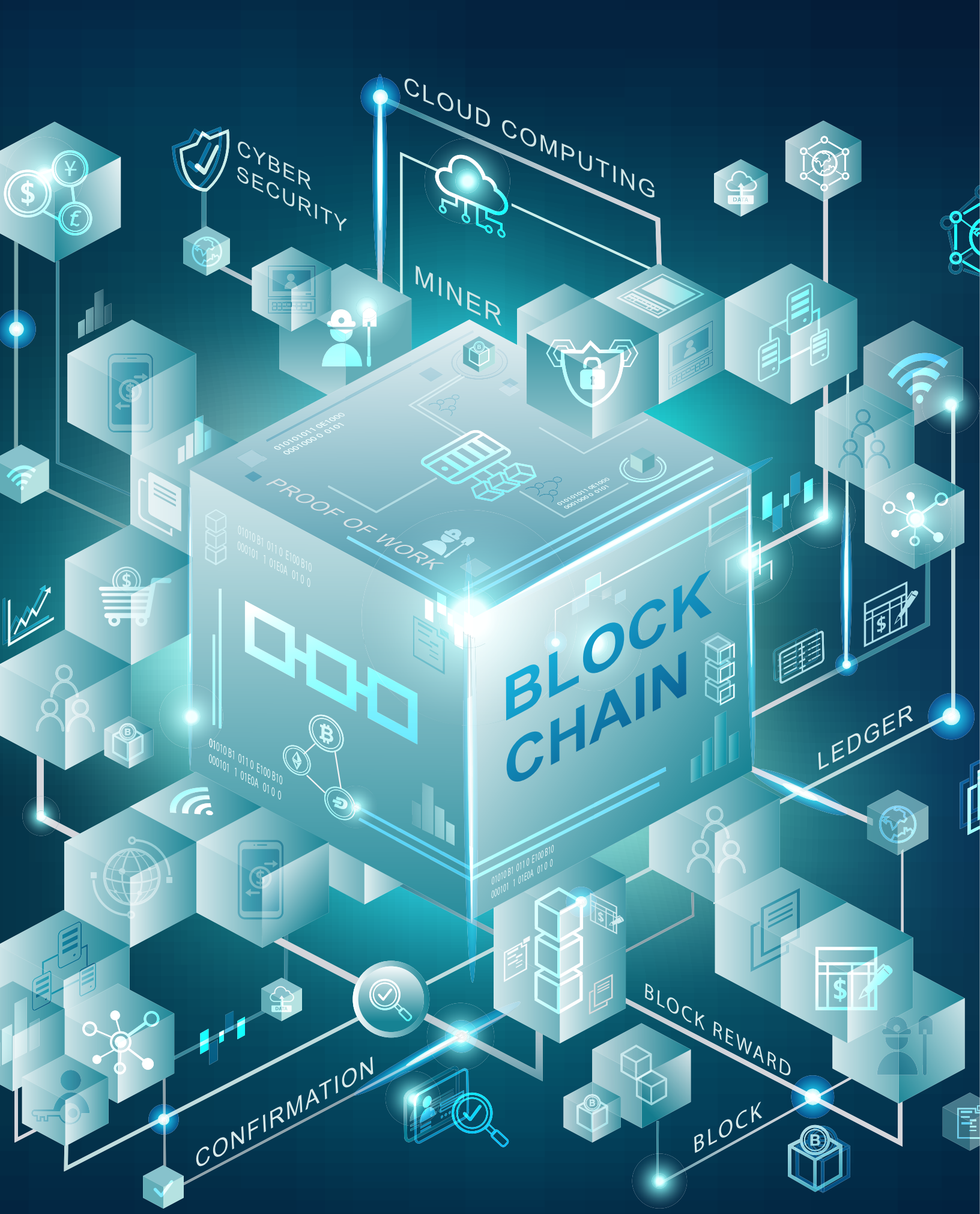


Figure 1 – Transaction storage in Corda

The foundational object of Corda is the state object which records an agreement between two or more parties documenting content and state. The ledger is a set of immutable state objects. Unlike Blockchains , Corda does not bundle transactions into a block, instead it persists/confirms transactions real time, and it does not boast of a native cryptocurrency.

Messages are delivered asynchronously using a Message Broker which facilitates better performance. Thus, Corda architecture allows for greater levels of Scalability to be achieved when desired.



IOTA:

IOTA is an open source permission-less distributed ledger built to power the future of Internet of Things.

The Distributed Ledger of IOTA is not a chain of blocks bundling transactions. Instead, it is based on Tangle – A Directed Acyclic Graph, a network of vertices joined by edges. Each vertex represents a transaction, the DAG grows only in one direction, hence "Directed". It is "Acyclic", since starting at any one vertex, the entire network cannot be traversed.

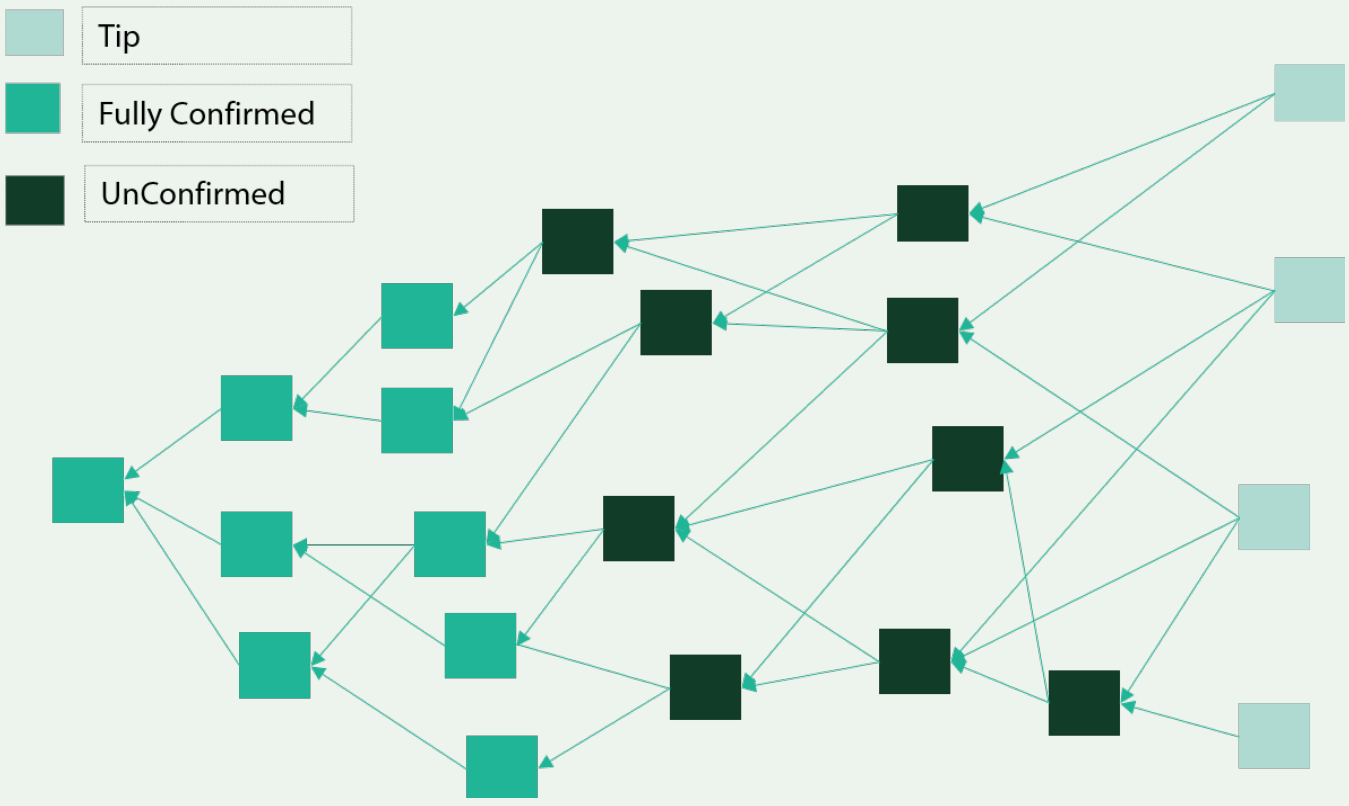
IOTA has no fees to transact and no scaling limitations; network transaction speed grows with activity. IOTA grows via transactors, not miners / stakers, thus avoiding centralization.

IOTA is aiming to be the backbone of the emerging machine-to-machine (m2m) economy of the Internet-of-Things (IoT), data integrity, micro-/nano- payments, and other cases where a scalable decentralized system adds value.

However, while it was intended to, IOTA is still not fully decentralized. The "Coordinator" node acts as a controller, with the objective to issue normal signed transactions called milestones. A transaction on IOTA is confirmed if and only if it is referenced by a milestone. Milestones set direction for growth of the Tangle.

IOTA was designed to counter the challenges around Proof of Work consensus algorithm, and instead works on a "Pay it Forward" Model. For each new transaction to be added to a Tangle as a vertex, it must validate 2 previous unvalidated transactions (vertices), that it will get hooked on to.

The true decentralization of IOTA , with elimination of the Coordinator node, is likely to lead to large scale adoption in the IOT space.



HASHGRAPH

Hashgraph is a DLT , that provides all features of Blockchain on one hand,– decentralization, transparency, provenance , while on the other , it alleviates drawbacks such as , Inefficiency of Proof of Work, Lack of fairness in Leader based consensus, and security challenges.

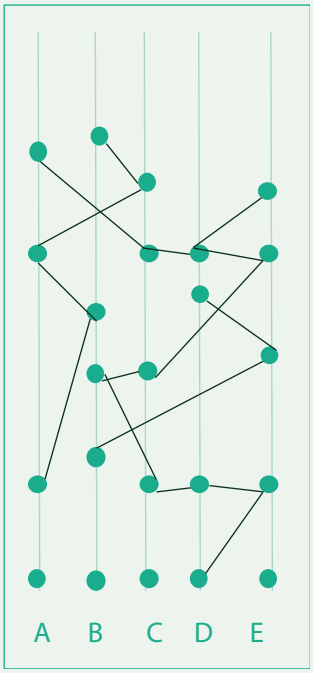
Hashgraph does not need miners to validate transactions and uses DAGs for adding transactions but does not record them in blocks. It uses the lightweight Gossip about Gossip protocol, and is able to proliferate transactions to other nodes exponentially.

The consensus mechanism leveraged by Hashgraph is actually a hybrid of Gossip and Voting algorithms:

Gossip about Gossip with Virtual Voting– Each node randomly talks to every other node, and shares all that they know, spreading data exponentially. When a node shares a transaction with another node, it also shares an audit trail of which node talked to which node (gossip about gossip) – which results in implicit voting, hence the term virtual voting.

How does it work:

A Hashgraph grows in one direction, and every participant node keeps a copy of the graph in its memory. One node calls another- the called node creates a new event that represents accumulation of transactions it is aware of. This cycle continues until all the nodes are aware of the information shared in a new event. Each event comprises of its timestamp of creation, the transaction details if any submitted at the node, the hash of self-parent (the previous event created on current node) and the hash of the other-parent (the last event from the other node), signed by the creator.



Each event contains the hashes of the events that occurred prior to it. This cumulative linking of events makes the graph immutable and hence cryptographically secure.

This builds a strong defense to malicious data theft or corruption, prevent manipulation of transaction data.

As a result of an implicit and lightweight consensus algorithms, Hashgraph offers tremendous scalability, to the tune of nearly 250k transactions per second.

Hashgraph is patented, not Open source.

Conclusion

The promise of DLTs offering unique solutions towards improving security, efficiency, and transparency is fast turning into reality. Several stakeholders across industry segments continue to invest in evolution of DLT technology to traverse the last lap towards comprehensive adoption.

While there is a motley of platforms springing up on the DLT horizon, there are a few that bring forth maturity and have the capability to truly disrupt status quo. Over the last year, R3's Corda DLT has emerged as a frontrunner, offering immense scalability, coupled with flexible consensus algorithms , and is especially suitable for Financial Services usecases. Among Blockchains, Hyperledger Fabric architecture was overhauled in its version 1.1 , bringing in architecture principles of Division of labor, with a diluted flavor of decentralization/democratization. The concept of Channels facilitated a reduced footprint and data sharing on need-to-know basis leading to better scalability and acceptability.

DAG based DLTs have brought about revolutionary changes in efficient scaling and low overheads. DAG brings distinct benefits of nearly limitless scalability, throughput that appreciates at the scale of activity, and varied options of Consensus.

As awareness grows, technologists continue to adapt and bring out newer flavors of DLT to blend with diverse business needs. The DLT revolution has come a long way since its genesis, and it is only a matter of time before we will witness large scale DLT adoption to scale across industries.

About the Author

Rohini Trehan
Delivery Manager - Financial Services, Infosys

Rohini has extensive delivery experience across Financial Services, leading large accounts, managing complex Systems Integration and Business Transformation programs. She has been instrumental in portfolio growth, building new practices and CoEs , providing strategic direction for accounts. In addition, she has been responsible for sustained delivery excellence, managing people and operations in her portfolio. She is passionate about technology , and also skilled in IT Strategy, Product Development, Project Governance, Agile Methodologies and Global Delivery.

She currently leads the Blockchain Center of Excellence and AMS practice for Financial Services at Infosys.

Rohini can be reached at Rohini_Trehan@infosys.com

References

- Ref 2- https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/ITU-Asia-Pacific-CoE-Training-on-Distributed-Ledger-Technologies-%28Blockchain%29-Ecosystem-and-Decentralization/Presentation.pdf
- https://thenextweb.com/hardfork/2018/07/27/distributed-ledger-technology-blockchain/
- https://thenextweb.com/hardfork/2018/07/24/google-blockchain-cloud-amazon/
- https://www.ccn.com/r3-consortiums-blockchain-initiative-what-makes-corda-different/
- http://www.corda.net/content/corda-technical-whitepaper.pdf
- www.iota.org
- https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd
- https://www.ledgerinsights.com/corda-enterprise-accenture-blockchain-winner/
- https://www.thewindowsclub.com/what-is-hashgraph
- https://www.happiestminds.com/insights/hashgraph/
- https://www.hedera.com/
- https://coinscenario.com/comparison-between-top-blockchain-platforms-and-protocols/