An Introduction to Distributed Ledger Technology

AlphaPoint

Executive Primer

An Introduction Distributed Ledger Technology

Company Background

AlphaPoint is a financial technology company that powers digital asset networks and provides institutions a Distributed Ledger Platform to digitize, trade, and manage the lifecycle of any asset. Its secure, scalable, and customizable platform enables customers to digitize assets, launch and operate markets, and reduce operational costs with its blockchain technology. AlphaPoint powers digital asset networks on 5 continents, and is led by a seasoned team with 150+ years in financial technology. AlphaPoint has offices in New York City, Philadelphia, and San Francisco.

What is DLT?

Distributed Ledger Technology, or blockchain, is a **new form of decentralized database**.

Strong cryptography ensures only designated parties can modify data held on the network.

Data is chunked into “blocks” that are “chained” together, giving the technology its name.

Why is it interesting?

The technology enables a series of technology **breakthroughs directly applicable to today’s financial markets**:

- Single truth
- Immutability
- Strong data governance
- Streamlined operations

How does it work?

The technology itself is **configurable per business needs**, and is at its core an efficient bundling of several well-known, time-tested concepts in computer science:

- Peer-to-peer networking
- Public key cryptography
- Distributed consensus

What is DLT?

A next-generation decentralized database…

"DLT" or "blockchain" denotes a shared digital ledger with **unique characteristics** –

- Eschews server-client model
- Each participant has its own copy of the database
- All changes are recorded, grouped into blocks, and verified by all peers
- This continuously-updated, tamper-proof database is called the blockchain

What is DLT?

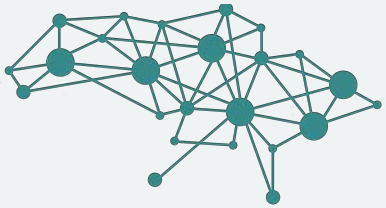
…with a novel coupling of characteristics…

- ✓ **Decentralized** – no single point of failure
- ✓ **Smart contracts** – certainty of code execution
- ✓ **Only designated parties** have control of given data
- ✓ **Pseudonymity** – not anonymity
- ✓ **Public verification** – irrefutable timestamping
- ✓ **Forward-only** – unalterable, though not unamendable

Why is it interesting?

…yielding a singular value proposition:

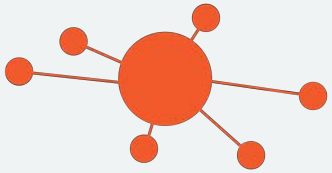
Decentralized network



In brief, blockchain offers a new model of verifiable trust –

- A single, immutable source of truth, with no single point of failure
- Existing across trust boundaries over any business network

Centralized network



By contrast, the status quo depends on trusted intermediaries running centralized databases -

- Single points of failure
- Complicated & costly - reconciliation, communication, security, et al.

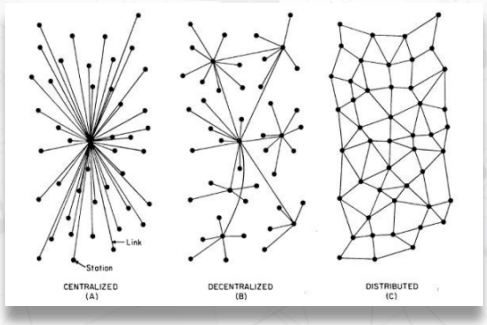
Distributed Ledger Technology – Technical Primer

AlphaPoint

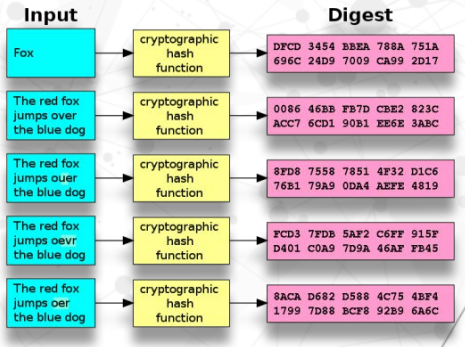
Technical Primer

Three Key Computing Concepts

Peer-to-Peer Networking



Public Key Cryptography



Distributed Consensus

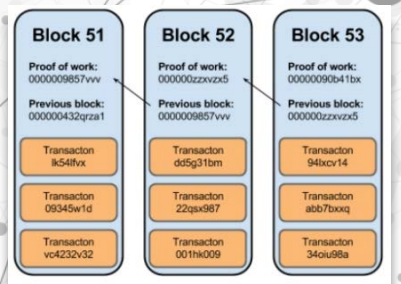


Image source: Wikimedia Commons

Technical Primer

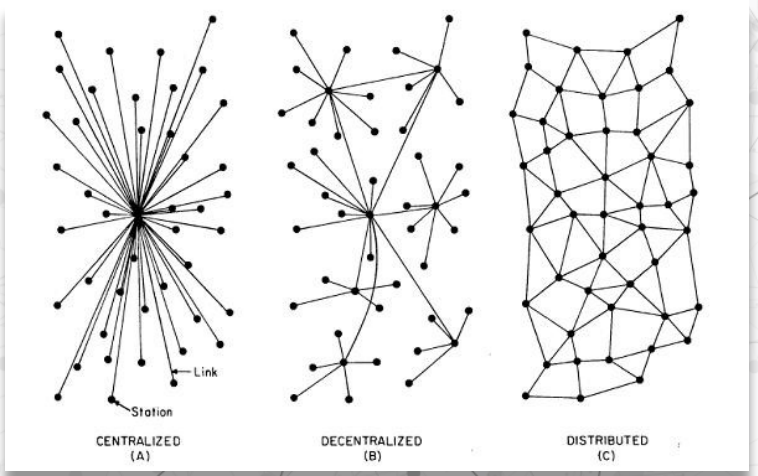
Peer-to-Peer Networking

Distributed network architecture undergirds blockchain:

- Peers are equally-privileged participants
- Popular examples of p2p systems include git, BitTorrent, or Bitcoin
- Solves “synchronization” problem in trustless environment

To reiterate: status quo is client-server model

- Single points of failure
- High-cost and complication



Technical Primer

Public Key Cryptography

Cryptographic Hashing

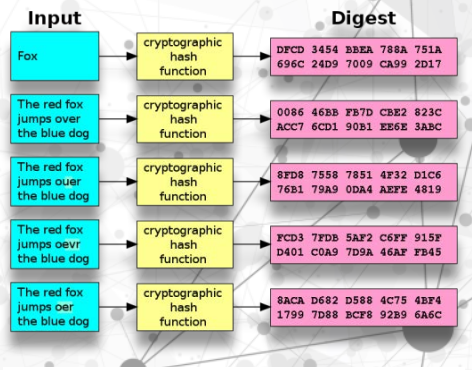
- Takes an input ('message') and returns a fixed-size output (‘digest’)
- One-way functions - easy to determine output from input, yet extremely hard to determine input from output

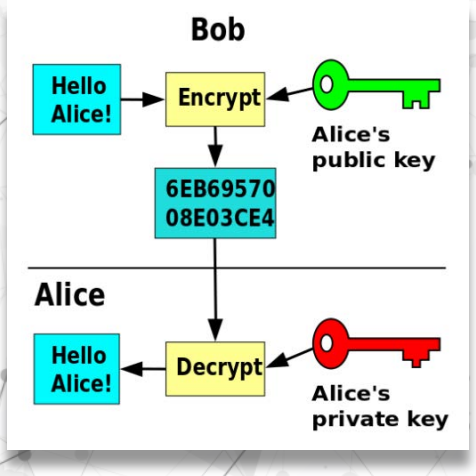
Public & Private Keys

- Message encrypted with a recipient's public key can only be decrypted by the recipient’s private key

Digital Signatures

- Authenticity of a message signed with sender's private key can be verified (but not accessed) by anyone who has the sender's public key





Technical Primer

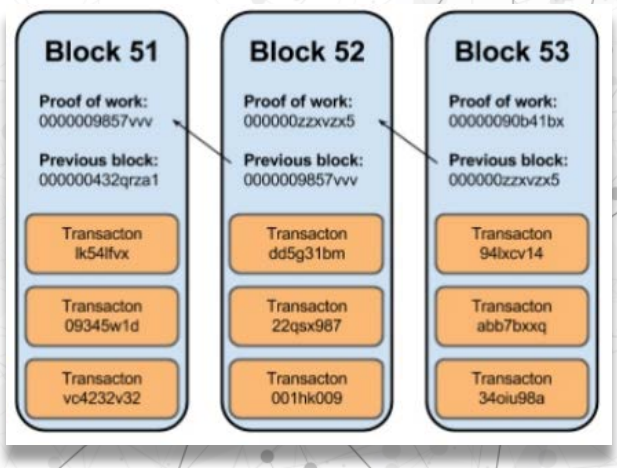
Distributed Consensus

Means by which network comes into agreement (‘achieves consensus’) about: [1] the global state of the database; & [2] veracity of additions thereto -

- Rules are baked into the protocol
- All blocks include a hash reference to the previous block – creating immutable chain
- Termed ‘mining’ or ‘confirming blocks’ in public ledgers

Different consensus mechanisms are optimized for different environments and use cases, e.g. -

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Proof of Elapsed Time (PoET)



Concepts in Action - Sample Transaction

	User Activity	Network Activity
1	**Alice** has a balance of 10 Tokens wants to send 1 Token to Bob – the Token may represent a loyalty point or a financial product.	Both Alice and Bob have a **public key** (or 'wallet address,' which acts as the **pseudonym**), as well as a secret **private key.**
2	Alice submits a message to the network, granting Bob access to a 1 Token balance.	Alice's message is signed with her private key and encrypted with Bob's public key. Only Bob can access the message / spend the Token. Yet the entire network can verify from **the output** that Alice (and no one else), was the signatory.
3	The message / position update is then broadcast to the entire network.	The message is relayed from node to node rapidly by **equally privileged peers** across the entire **peer-to-peer network**.
4	Transaction processors verify the message, and include it in the latest block – Alice's transaction is now **confirmed**.	Transactions, if valid, are included in the new block, along with a reference to the previous block, ensuring the immutability of all prior blocks.

Concepts in Action - Sample Transaction

	User Activity	General Blockchain Truisms
1	**Alice** has a balance of 10 Tokens wants to send 1 Token to Bob – the Token may represent a loyalty point or a financial product.	Only appropriate parties have access to modify underlying data.
2	Alice submits a message to the network, granting Bob access to a 1 Token balance.	All messages are protected by strong cryptography.
3	The message / position update is then broadcast to the entire network.	Messages are broadcast across the entire network.
4	Transaction processors verify the message, and include it in the latest block – Alice's transaction is now **confirmed**.	The network comes into agreement on 'global state.'

How & When to Build on DLT

AlphaPoint

When to Build on DLT

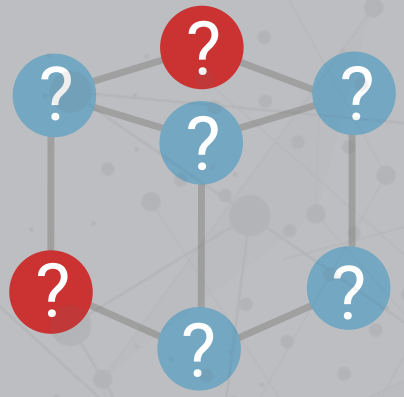
Value Proposition for Financial Services

Value drivers in financial services are drawn from private/permissioned “activity ledgers”, rather than public “asset ownership” ledgers – foremost include:

- ✓ Operational simplification
- ✓ Regulatory efficiency
- ✓ Counterparty risk reduction
- ✓ Clearing and settlement latency
- ✓ Liquidity and capital improvement
- ✓ Fraud reduction

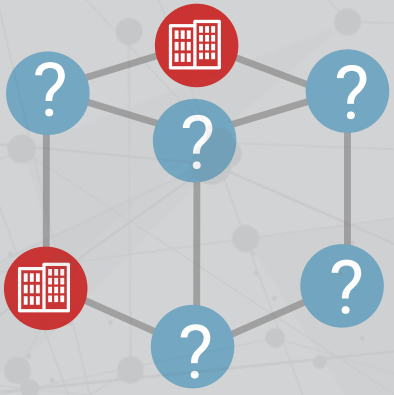
List source: World Economic Forum

Public Blockchain



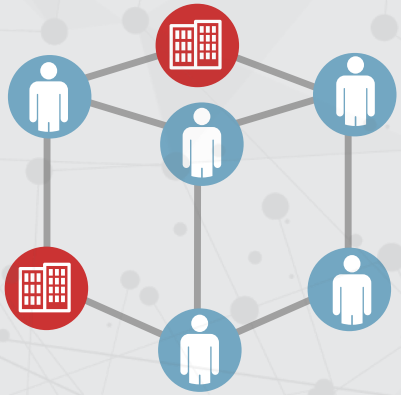
Ledger is **fully open to public participation**. All users and and transaction validators are pseudonymous.

Federated Blockchain



Ledger remains open to public access, **but transactions are validated by known parties**.

Permissioned Blockchain



Ledger access is restricted to positively identified users. **Most appropriate for high-value, sensitive markets and assets.**

Technical Primer

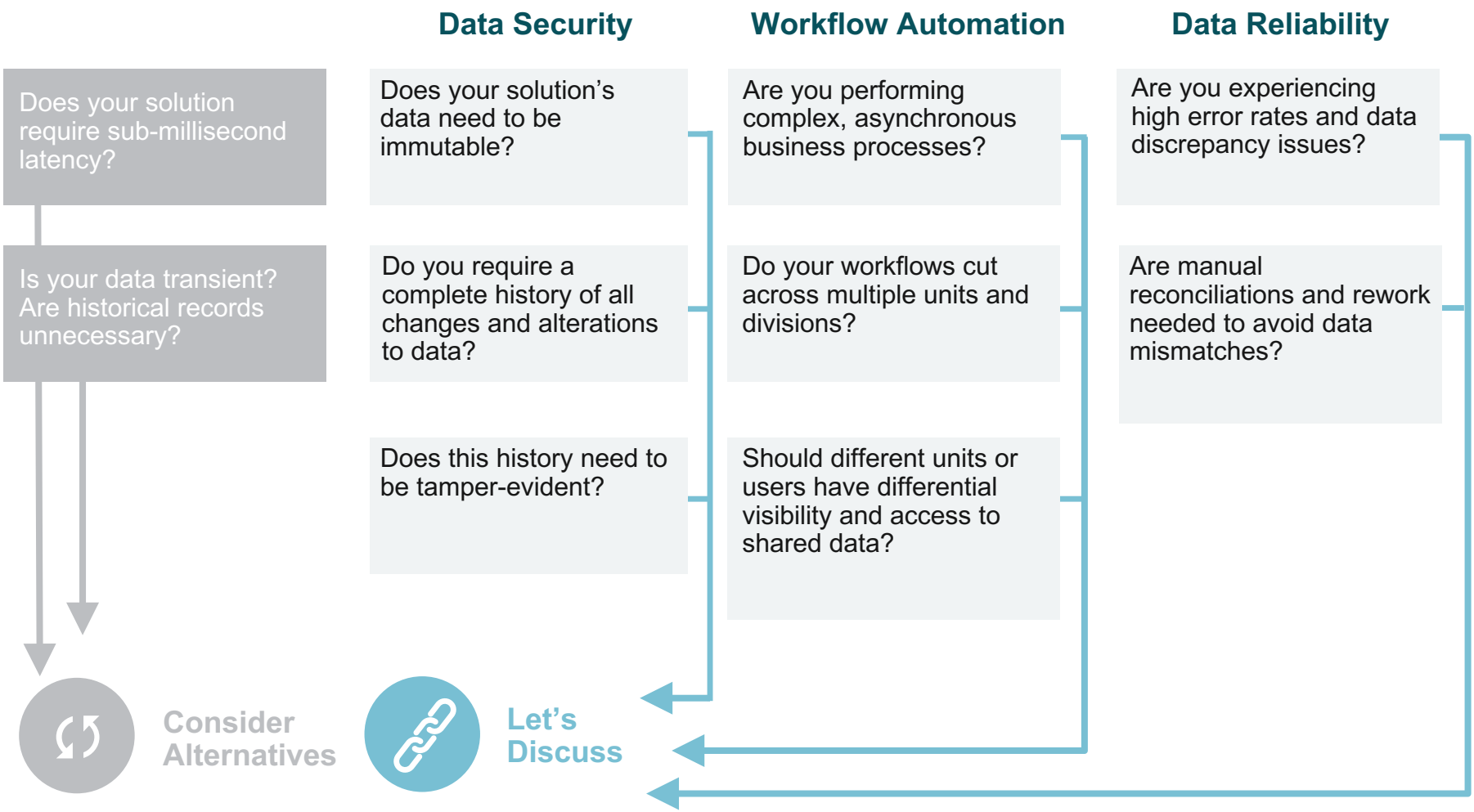
“Ownership” vs. “Activity” Ledgers

	“Asset Ownership Tracking”	“Activity Register”

What is being tracked?	▪ Changes of ownership of digital tokens
	▪ Tokens may be actual assets (e.g. BTC, XRP)
	▪ Tokens may also represent claims
		▪ Immutable timestamped data records
		▪ Underlying data can be anything -
		  ▪ Trade Facts
		  ▪ Identity information
		  ▪ Newspaper headline
		  ▪ Picture

What does Consensus denote?	▪ Network agrees said ownership changes are valid as per network rules ▪ Network stores changes in ownership	Two categories for consensus - ▪ **Relevant party consensus**, i.e. one or more parties agree on the content of some data ▪ **Network consensus**, i.e. validating parties agree that the existence of data has been legitimately uploaded

When to Build on DLT



Next Steps

To learn more about how Distributed Ledger Technology can transform your business or market, please reach out to our team at -

info@alphapoint.com

Or schedule a platform demo at -

alphapoint.com

AlphaPoint