# Unpacking the Blockchain

Matthew Savare
Partner

Lowenstein Sandler

# Unpacking the Blockchain

April 25, 2018

Matthew Savare, Esq.

Lowenstein Sandler

# Blockchain or Distributed Ledger Technology

## What is DLT?

- DLT, or blockchain, is a **new form of decentralized database**.
- Strong cryptography ensures only designated parties can modify data held on the network.
- Transaction 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

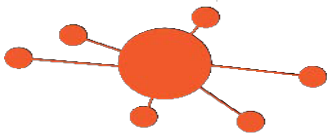
# Why is it Interesting?
# …yielding a singular value proposition:

**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

Decentralized network

Centralized network



**By contrast, the status quo depends on trust intermediaries running centralized databases** –

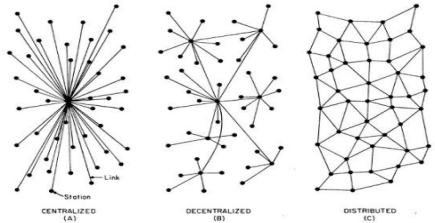
- Single points of failure
- Complicated & costly – reconciliation, communication, security, et al.

# Distributed Ledger Technology – Technical Primer

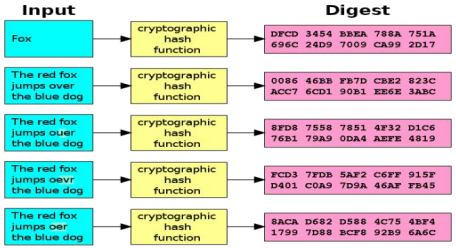
Lowenstein Sandler

# Technical Primer
# Three Key Computing Concepts

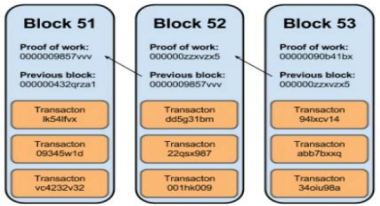
## Peer-to-Peer Networking




## Public Key Cryptography




## Distributed Consensus



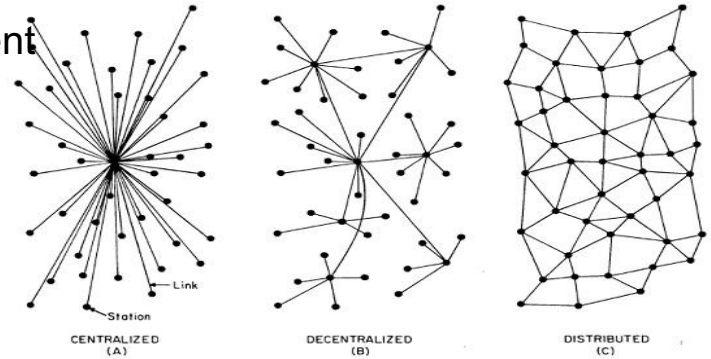
# Technical Primer
# Peer-to-Peer Networking

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

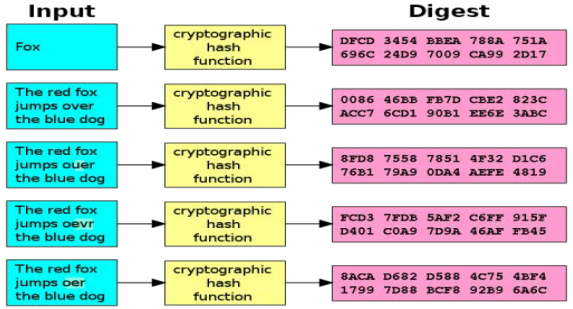
- Takes an input ('message') and returns a fixed-size output (‘digest’)
- One-way functions - easy to determine output from input, yet extremely hard to determine input from output

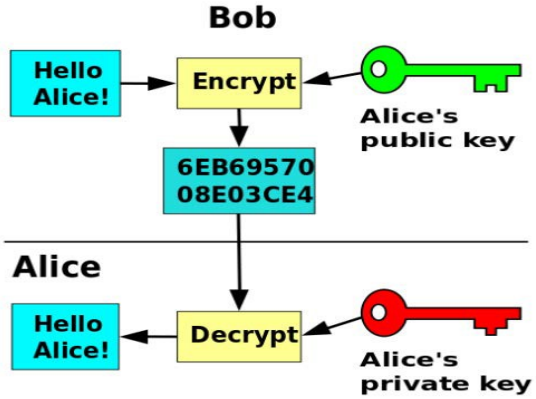
## Public & Private Keys

- 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

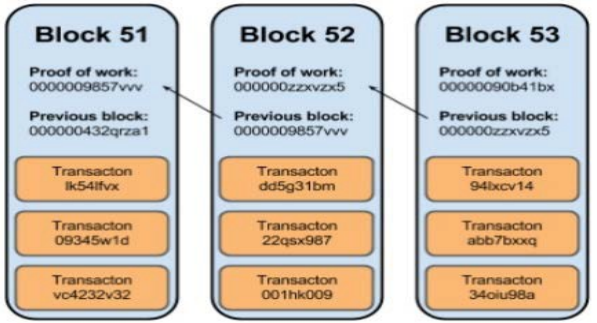


# Technical Primer
# Distributed Consensus

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

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.
2. Alice submits a message to the network, granting Bob access to a 1 Token balance.
3. The message / position update is then broadcast to the entire network.
4. Transaction processors verify the message, and include it in the latest block – Alice's transaction is now **confirmed**.

## Network Activity

1. 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'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 is relayed from node to node rapidly by **equally privileged peers** across the entire **peer-to- peer network**.
4. 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

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.
2. Alice submits a message to the network, granting Bob access to a 1 Token balance.
3. The message / position update is then broadcast to the entire network.
4. Transaction processors verify the message, and include it in the latest block – Alice's transaction is now **confirmed**.

## General Blockchain Truisms

1. Only appropriate parties have access to modify underlying data
2. All messages are protected by strong cyptography
3. Messages are broadcast across the entire network
4. The network comes into agreement on 'global state.'

# An Introduction to Cryptocurrencies

Lowenstein Sandler

# What is Virtual or Cryptocurrency?

- **Virtual currency** is a "digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status … in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency." Financial Action Task Force.
- Different from **fiat currency** (a.k.a. **"real currency," "real money,"** or **"national currency"**) and e**-money**, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency.

# Types of Cryptocurrencies

- Well over 1,500 virtual currencies
- Bitcoin
  - released in 2009 by Satoshi Nakamoto;
  - first decentralized ledger currency;
  - most popular with highest market capitalization.
- Bitcoin Cash
  - hard fork from Bitcoin
- Ether
  - Supports smart contracts
- Ripple
- Litecoin

# Initial Coin Offerings

# What in an ICO?

- Fundraising event in which an entity offers participants a unique coin or token in exchange for consideration (usually Bitcoin or Ether).
- Tokens are issued on a blockchain and entitle holder to certain rights:
  - Profits
  - Shares of assets
  - Rights to use a product or service
  - Voting rights
- ICOs are typically announced online through whitepapers.

# Business and Legal Challenges

- Since 2011, at least 36 heists of cryptocurrency exchanges with more $4 billion dollars of Bitcoins stolen.
  - Mt. Gox
  - Moolah
- Government intervention
  - China bans ICOs and orders cryptocurrency exchanges to stop trading
  - South Korea bans ICOS
  - SEC charged pair of ICOs (Recoin and DRC World) with fraud.
- Flash crashes and wild price fluctuations
  - When Kraken was under cyber attack, Ether dropped 70%
- Certain exchanges do little diligence on their customers
  - Money laundering
  - Sanctions violations

# Lowenstein Sandler Core Values

## OUR CORE VALUES MAKE US DIFFERENT.
## WHAT MAKES US DIFFERENT MAKES US SUCCESSFUL.

We are committed deeply to **client service**.

We honor the **trust** others have placed in us.

We are **entrepreneurial**.

We **anticipate** rather than merely respond.

We are **passionate** about everything we do.

We encourage **creativity** to flourish.

We are **generous** with our time and our talent.

We work to **connect** clients and communities.

# STAY CONNECTED


lowenstein.com