Blockchain Overview
History

1991: The first crypto secured chain of blocks
How to time-stamp a digital document

1991

2008

Bitcoin Author
The first blockchain Implementation
Bitcoin Cash Systems paper

2014: MIT Bitcoin Club
The first blockchain clubs that continuously strives to educate members blockchain

2014/2015

2015:
The first peer reviewed academic journal dedicated to cryptocurrency and blockchain technology research, Ledger, was announced

2015: The first blockchain Innovation Center in Singapore

2015 ...

2015: Linux Foundation announced Hyperledger
2015: Ethereum first release.
2015: R3 Consortium.
World Economic Forum group started to put the governance model of Blockchain
What is Blockchain?

Abstract Theory

Any participant in the network to see THE system of record (ledger)
P2P network
Hash: e2c521bc53bb5db4fc0aa497da2ba5d4c8444db3
Hash of previous block

Creates the chain!
Hash: 1Z8F  
Previous hash: 0000

Hash: 6BQ1  
Previous hash: 1Z8F

Hash: 3H4Q  
Previous hash: 6BQ1
What is Blockchain?

Broader participation
lower cost
increasing efficiency

Business Perspective

What

Immutable

Shared ledger

Business terms embedded in the database

Smart contract

Privacy

Appropriate visibility
Securing the transactions

Consensus

All parties agree to network verified transaction
Business Networks

- Business Networks
  Benefit from connectivity
  - Participants are
    - Customers
    - Suppliers
    - Banks
    - Partners
  - Cross geography & regulatory boundary
Shared ledger

Records all transactions across business network

- Shared between participants
- Participants have own copy through replication
- Permissioned or Permissionless
- THE shared system of record
**Centralized**  

**Decentralized**  

**Distributed Ledgers**  

---  

**The New Networks**  

Distributed ledgers can be public or private and vary in their structure and size.  

- Users (●) are anonymous  
- Users (●) are not anonymous
Ledgers are key ...

**Ledger** is THE system of record for a business. Business will have multiple ledgers for multiple business networks in which they participate.

- **Transaction** – an asset transfer onto or off the ledger
  - John gives a car to Anthony (simple)

- **Contract** – conditions for transaction to occur
  - If Anthony pays John money, then car passes from John to Anthony (simple)
  - If car won't start, funds do not pass to John (as decided by third party arbitrator) (more complex)
Smart contract

Business rules implied by the contract … embedded in the Blockchain and executed with the transaction

• Verifiable, signed
• Encoded in programming language
Consensus

... the process by which transactions are verified

- When participants are anonymous
- Multiple alternatives

**Proof of Work**, Bitcoin cryptographic mining provides verification for anonymous participants but at significant compute cost.

- **Proof of Stake** where fraudulent transactions cost validators (e.g. transaction bond)
- **Multi-signature** (e.g. 3 out of 5 participants agree)
- **PBFT** (cross checked secure message exchange)
Ledger is shared, but participants require privacy

- Participants need:
  - Transactions to be private
  - Identity not linked to a transaction

- Transactions need to be authenticated

- Cryptography central to these processes
Transferring assets, building value

Anything that is capable of being owned or controlled to produce value, is an asset.

Two fundamental types of asset
- Tangible, e.g. a house
- Intangible, e.g. a mortgage

Intangible assets subdivide
- Financial, e.g. bond
- Intellectual, e.g. patents
- Digital, e.g. music

Cash is also an asset
- Has property of anonymity
Problem ...

... Inefficient, expensive, vulnerable
Solution …

Shared, replicated, permissioned

… Consensus, provenance, immutability, finality

Party A’s records
Party B’s records
Party C’s records
Party D’s records
Bank records
Auditor records
Blockchain benefits

**Saves time**
Transaction time from days to near instantaneous

**Removes cost**
Overheads and cost intermediaries

**Reduces risk**
Tampering, fraud & cyber crime

**Increases trust**
Through shared processes and recordkeeping
Blockchain use cases are too many.
Food Trust Solutions built on Blockchain technology

_one in 10 people_ around the world become ill due to foodborne diseases every year.

_~420,000 of them die._

because it takes far too long to isolate product recall or contamination issues in the supply chain.

Blockchain is used to create a trusted connection with shared value for all ecosystem participants, including end consumers

The solution offers connectors for interoperability and leveraging existing standards (e.g., GS1)

Trust is a fragile thing. Break it even once, and people will never forget.
The effectiveness of the IBM Food Trust solution was demonstrated with a Walmart mango pilot.

**Pilot Test Case**

How long does it take to trace a package of sliced mangoes back to the farm?

**Supply Chain**

**Results**

Typical manual, mixed digital and paper-based method:
- 6 days
- 18 hours
- 26 minutes

IBM Food Trust Track and Trace digital solution:
- 2.2 seconds
<table>
<thead>
<tr>
<th>What</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Competitors/collaborators in a business network need to share</td>
<td>1. Consolidated, consistent dataset reduces errors</td>
</tr>
<tr>
<td>reference data, e.g. bank routing codes</td>
<td>2. Near-real-time of reference data</td>
</tr>
<tr>
<td>• Each member maintains their own codes, and forwards changes to</td>
<td>3. Naturally supports code editing and routing code transfers between</td>
</tr>
<tr>
<td>a central authority for collection and distribution</td>
<td>participants</td>
</tr>
<tr>
<td>• An information subset can be owned by organizations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>How</td>
<td></td>
</tr>
<tr>
<td>• Each participant maintains their own codes within a Blockchain</td>
<td></td>
</tr>
<tr>
<td>network</td>
<td></td>
</tr>
<tr>
<td>• Blockchain creates single view of entire dataset</td>
<td></td>
</tr>
</tbody>
</table>
Finality use case – Letter of credit

**What**
- Bank handling letters of credit (LOC) wants to offer them to a wider range of clients including startups
- Currently constrained by costs & the time to execute

**How**
- Blockchain provides common ledger for letters of credit
- Allows all counter-parties to have the same validated record of transaction and fulfillment

**Benefits**
1. Increase speed of execution (less than 1 day)
2. Vastly reduced cost
3. Reduced risk, e.g. currency fluctuations
4. Value added services, e.g. incremental payment
Provenance use case – Vehicle maintenance

**What**
- Provenance of each component part in complex system hard to track
- Manufacturer, production date, batch and even the manufacturing machine program

**How**
- Blockchain holds complete provenance details of each component part
- Accessible by each manufacturer in the production process, the aircraft owners, maintainers and government regulators

**Benefits**
1. Trust increased, no authority "owns" provenance
2. Improvement in system utilization
3. Recalls "specific" rather than cross fleet
### Immutability use case – Financial ledger

**What**
- Financial data in a large organization dispersed throughout many divisions and geographies
- Audit and Compliance needs indelible record of all key transactions over reporting period

**How**
- Blockchain collects transaction records from diverse set of financial systems
- Append-only and tamperproof qualities create high confidence financial audit trail
- Privacy features to ensure authorized user access

**Benefits**
1. Lowers cost of audit and regulatory compliance
2. Provides “seek and find” access to auditors and regulators
3. Changes nature of compliance from passive to active
## Blockchain Platforms

<table>
<thead>
<tr>
<th></th>
<th>Ethereum</th>
<th>Hyperledger</th>
<th>R3 Corda</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Industry / Purpose</strong></td>
<td>Cross / B2C</td>
<td>Cross / B2B</td>
<td>Financial / B2B</td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>Ethereum Developers</td>
<td>Linux Foundation</td>
<td>R3 Consortium</td>
</tr>
<tr>
<td><strong>Ledger Type</strong></td>
<td>Permissionless</td>
<td>Permissioned</td>
<td>Permissioned</td>
</tr>
<tr>
<td><strong>Cryptocurrency</strong></td>
<td>Ether (ETH)</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>Consensus</strong></td>
<td>PoW</td>
<td>Pluggable (RBFT)</td>
<td>Pluggable</td>
</tr>
<tr>
<td><strong>Language</strong></td>
<td>Solidity</td>
<td>Go / Java</td>
<td>Kotlin</td>
</tr>
</tbody>
</table>
Summary

Blockchain …

– is a shared, replicated, distributed ledger technology
– can open up business networks by taking out cost, improving efficiencies and increase accessibility
– addresses an exciting and topical set of business challenges, which cross every industry
Thank you!