Blockchain and Cryptocurrencies
The potential to rewire financial services and other systems?

Steven Shafer
Treasury Management Sales Consultant

May 22, 2018
A brief history of blockchain and distributed ledger technology

2008
- Bitcoin whitepaper introduces blockchain
  “Peer to peer electronic cash and payment system”

2009
- Open source project and social movement around launching the Bitcoin blockchain

2010
- First Bitcoin exchange founded, and the open trading of cryptocurrency is established

2012
- Wells Fargo conducts formal research on Bitcoin

2014
- Wells Fargo publishes Bitcoin 101 paper
  *Wells Fargo concludes no interest in this cryptocurrency*

2015
- Focused technical research on blockchain and distributed ledger technology (DLT)

2016
- Industry consortiums begin co-developing DLT solutions

2018
- Industry is focused on delivering commercial solutions using DLT
What is blockchain?

- A blockchain is a distributed ledger of transactions that have been validated through a consensus mechanism between members in a network.

- Transactions are chronologically grouped into blocks of data, each cryptographically linked to predecessor transactions down to the genesis block, thereby creating a chain of blocks.

- Since each block draws upon the "hashed" data reference of the previous block in the chain, it is virtually impossible to add, remove or change data without being detected by other members in the network.
How does a blockchain work?

**Current Blockchain**

- Transaction 999
- Transaction 998
- Transaction 997
  - Reference to Prior Block

- Transaction 996
- Transaction 995
- Transaction 994
  - Reference to Prior Block

- Transaction 993
- Transaction 992
- Transaction 991
  - Reference to Prior Block

**Adding a New Block**

- **Record** recent transactions in the network, each with a timestamp, and bundle them into a block, also with a timestamp and with a reference to the prior block.

- **Secure** the block in the network using cryptography and computing power to create a “hash” that represents the data, and verify it to prove that the prior hashes all match up and therefore the new block hash is legitimate.

- **Add** the new block to the chain and distribute it to the network as appropriate.

**Updated Blockchain**

- Transaction 1,002
- Transaction 1,001
- Transaction 1,000
  - Reference to Prior Block

- Transaction 999
- Transaction 998
- Transaction 997
  - Reference to Prior Block

- Transaction 996
- Transaction 995
- Transaction 994
  - Reference to Prior Block
Blockchain versus Distributed Ledger Technology (DLT)

- A blockchain is just one type of distributed ledger, and not all distributed ledgers necessarily employ blocks or chain transactions.
- A distributed ledger is comprised of three core technologies combined in different arrangements depending upon the use case.
  - **Cryptography** – securely validates identity, permissions and transactions on the network
  - **Distributed data storage** – ensures shared view of the same data and eliminates the need for reconciliation
  - **Peer-to-peer networking** – connects participants to shared data in real time
Why DLT?
Centralized Ledger

- Transactions are recorded by a central, trusted authority maintaining a centralized ledger that must be reconciled with each participant's copy of the ledger.
  - Limited visibility into business records due to multiple non-standard data sources and external parties also with multiple sources of data.
  - Inter-transaction dependencies which need to be verified due to central administrator and SOR.
  - Lack of data standards and security of data in reconciliation processes.
Why DLT?
Distributed Ledger

- Transactions are recorded on a common, shared ledger and confirmed by participants in real time, thus creating trust in the network and eliminating the need for reconciliation
  - Removes intermediary parties to settlement, saving time and reducing operational expense
  - Records are committed only once consensus is achieved thus eliminating reconciliation, and creating a reusable trusted source of data
  - Greater security with “immutable records” such that the system itself can be used for irrefutable evidence and regulatory scrutiny
DLT examples: financial services

Global Payment Services

Improve operations around cross currency exchange of value to reduce risk.

Lending & Trade Finance

Open new markets in trade finance with better financial terms than currently exist.

Investment Banking and Capital Markets

Reduce or remove the need for many post-settlement operations, and add efficiencies of scale; explore tokenization to increase asset utility.

Identity Services

Improve client engagement and experience with mutualized internal customer data management.
DLT examples: other companies

**Cross Border Payments**
Improve operations around cross currency exchange of value to reduce risk.

**Smart Contracts**
Executes contracts publically stored while maintaining privacy of the individuals involved.

**Shared Data**
Sharing Healthcare and Food distribution information across borders, both inter and intra-company; i.e. tracing a head of lettuce from the grocery store back to the specific source farm.

**Personal Identification Records**
Validate specific driver’s license and passport information.
An option contract between parties is written as code into the blockchain. The individuals involved are anonymous, but the contract is the public ledger.

A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors’ positions.
A brief history of currency - value stores and transfer mechanisms

- **Barter**: 9000-6000 BCE
- **Cattle, Grain**: 806
- **Metal Coins**: Roman Empire
- **Paper Currency**: China
- **The Gold Standard**: England 1816, United States 1900
- **Freely floating fiat in US**: 1971
- **Early explorations of centralized digital currency end in tears**:
  - 1983-98 DigiCash
  - 1998-2005 eGold
  - 2005 QCoins
  - 2006 Liberty Reserve
- **Bitcoin**: decentralized, autonomous, solves for double spend but not governance
- **180 sovereign fiat currencies**: Approximately 147 (and growing!) for profit cryptocurrencies

Early History 9000-6000 BCE 1000 BCE 806 1816-1900 1971 1983-2006 2008 2018
What is next for currency?
The Money Flower: A Taxonomy of Money

Source: https://www.bis.org/publ/qtrpdf/r_qt1709z.htm
What is next for currency?
The Money Flower: Examples Past, Present and **Future**

Source: https://www.bis.org/publ/qtrpdf/r_qt1709z.htm

A standard font indicates that a system is in operation; an *italic* font indicates a proposal; an *italic and underlined* font indicates experimentation; a strikethrough font indicates a defunct company or an abandoned project.

Source: https://www.bis.org/publ/qtrpdf/r_qt1709z.htm
Bitcoin transfer: Blockchain example
Key considerations around cryptocurrencies

- **Digital assets** and not currencies
  - Value token: Bitcoin, Ether, LiteCoin, etc.
  - Utility token: Used to enable access to services
  - Equity token: Acts as a security investment
- 100% speculation
- Extremely volatile
- Intensive integration required for point of sale or accounts receivables/payables transactions
- Central Bank Digital Currency (CBDC) will eventually emerge, with negative impact on current cryptocurrencies without similar governance or backing
What is the potential path to legitimacy for cryptocurrencies or any tokenized asset?

- New Avenues for Value Exchange?
  - Autonomous units of value, for a global audience that wants unlimited access to a fungible digital asset
  - Universal Payment Network, in production for cross border remittances via the Stellar Network
  - xRapid, a possible new RTGS or cross border remittance platform
  - A potential front runner DLT platform for a central bank digital currency (CBDC)
  - Utility Settlement Coin (USC) Project, for tokenized depository receipts at central banks

- Value Stores?
  - ICOs – Intended for access to distributed application services; sadly being wildly misused [www.deadcoins.com](http://www.deadcoins.com)
  - Tokenized assets – Potential to create liquidity, like digitized paper-based securities

- Value Exchange and Store?
  - Open market crypto exchanges vs Central Bank Digital Currency
Other cryptocurrencies

- Ethereum
- Bitcoin Cash
- Ripple
- Litecoin
- Dash
- IOTA
- Monero
The thing about bubbles – they can hang out there for a while...

Sea South

Gouda Tulip Bulbs

Bitcoin
Evolution of Trust and Architectures

**Internal Transaction Systems**
- **Architecture**: Centralized internal database (e.g. IBM, Oracle)
- **Settlement Process**: Internal
- **Speed**: Real-time
- **Transaction Cost**: Internal
- **Benefits**: Speed, cost and (relative) simplicity
- **Limitations**: Committing transactions with third parties/across network

**Middleware/ Messaging**
- **Architecture**: Secure inter-party messaging/queue-based middleware
- **Settlement Process**: Independent (but enabled by messaging)
- **Speed**: Up to 3-5 days
- **Transaction Cost**: External provider + settlement costs
- **Benefits**: Secure transaction between external parties, standardized data formats
- **Limitations**: Data errors slow transactions, flexibility

**Clearing Houses**
- **Architecture**: Third party agent-in-possession
- **Settlement Process**: Via clearing house
- **Speed**: Days (transaction dependent)
- **Transaction Cost**: Third-party service
- **Benefits**: Reduced settlement risk/DVP
- **Limitations**: Complex and cumbersome, expensive

**Blockchain**
- **Architecture**: Distributed ledger with cryptographic integrity
- **Settlement Process**: Consensus
- **Speed**: Near real-time to minutes
- **Transaction Cost**: Similar to internal databases
- **Benefits**: Enables third-party transaction to be as simple and efficient as internal transactions
- **Issues**: Tech maturity, integration with existing systems/workflows

Source: Magister Advisors
<table>
<thead>
<tr>
<th>Concept</th>
<th>Bitcoin</th>
<th>Ethereum</th>
<th>Fabric</th>
<th>Corda</th>
<th>Quorum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blockchain and/or Distributed Ledger</strong></td>
<td>One blockchain containing all transactions, there are no states</td>
<td>One blockchain containing all transactions and states</td>
<td>Multiple blockchains containing all transactions and states which can be segregated into channels, with each channel having its own ledger</td>
<td>A decentralized database solution but not a blockchain, because by design data is not propagated to all network participants and is not stored in blocks</td>
<td>One blockchain containing all transactions in the Public state, where each member also maintains a unique Private state about transactions in which it participates</td>
</tr>
<tr>
<td><strong>Consensus Mechanism</strong></td>
<td>Proof of Work, with mining</td>
<td>Proof of Work, with mining</td>
<td>Kafka, with other options pluggable</td>
<td>Notaries, with other options pluggable</td>
<td>Public: Proof of Work, with mining Private: RAFT and BFT</td>
</tr>
<tr>
<td><strong>State Tracking Model</strong></td>
<td>Stateless, UTXO</td>
<td>Account-based and with states</td>
<td>Agnostic, but uses ordering service with endorsers</td>
<td>Transaction-based with UTXO, and a Notary service</td>
<td>Account-based and with states</td>
</tr>
<tr>
<td><strong>Data and Transaction Management</strong></td>
<td>Federally decentralized</td>
<td>Federally decentralized</td>
<td>Channels – assets are on a pre-defined list of selected peers, no one leaves and no ones joins without considerable configuration effort</td>
<td>Flows – states and messages and other network traffic only travels between nodes connected point to point and which are only ‘need to know’, and a Vault is used to store data</td>
<td>States – Public and Private data are managed separately, with payloads only distributed to transacting parties</td>
</tr>
<tr>
<td><strong>Smart Contracts</strong></td>
<td>No</td>
<td>Yes, called Smart Contracts, written in Solidity</td>
<td>Yes, called Chaincode, written in GoLang</td>
<td>Yes, called Smart Contracts, written in Kotlin or Java</td>
<td>Yes, called Smart Contracts, written in Solidity</td>
</tr>
<tr>
<td><strong>Native Assets</strong></td>
<td>Bitcoins are the byproduct of mining for the consensus logic, intended to create virtuous action by all participants without requiring trust</td>
<td>Ether is the byproduct of mining for the consensus logic, intended to create virtuous action by all participants without requiring trust</td>
<td>No native asset</td>
<td>No native asset</td>
<td>No native asset</td>
</tr>
<tr>
<td><strong>Network Type</strong></td>
<td>Permissionless</td>
<td>Permissionless</td>
<td>Permissioned</td>
<td>Permissioned</td>
<td>Permissioned</td>
</tr>
<tr>
<td><strong>Participant Management</strong></td>
<td>Anyone can join</td>
<td>Anyone can join</td>
<td>Each participant is managed via X.509 certificates by default, with additional policies that can govern what each can do on the network</td>
<td>Each participant is managed via X.509 certificates</td>
<td>Each node maintains a permissioned-nodes.json file, with a role of: Maker and/or Voter, or Observer</td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>None</td>
<td>Ethereum Foundation, a Swiss nonprofit</td>
<td>Linux Foundation, a 501(c)(6) nonprofit</td>
<td>R3</td>
<td>JPM</td>
</tr>
</tbody>
</table>
References

https://digital.wf.com/treasuryinsights/portfolio-items/tm13039/

https://p1xhr2w8ts37fbalioe6qfro-wpengine.netdna-ssl.com/treasuryinsights/wp-

https://www.youtube.com/watch?v=SSo_EIwHSd4

https://youtu.be/lik9aaFIsl4

https://youtu.be/kubGCSj5y3k

https://youtu.be/-mgxEhIvSTY

https://global.delaware.gov/2016/06/10/the-delaware-blockchain-initiative-potential-
amendments-to-the-delaware-general-corporation-law/