Formally: An informal introduction to Blockchain

Disclaimer

- This is not a Bitcoin introduction. This is a high-level introduction to Blockchain technology. However, we should acknowledge that Satoshi Nakamoto (pseudonym) and his/their creation, Bitcoin, popularized Blockchain technology. (There are currently arguments that Bitcoin was not the first blockchain.)
- Today there are various *flavors* of Blockchain. This paper attempts to generalize Blockchain with samples in some of those flavors. Additional research, prototyping, and due diligence should be exercised before making any long-term decisions.
- Lastly, it is the opinion of the author, no single Blockchain solution will fulfill all needs. As many of the Blockchain technologies are paradigm specific, one should educate themselves on when and how to implement a Blockchain solution. Perhaps more importantly, when NOT to implement a solution.

A Brief history of Blockchain

- On October 31, 2008, *Satoshi Nakamoto* released the Bitcoin White Paper outlining a purely peer to peer electronic cash/digital asset transfer system. This is the first popular implementation of Blockchain and is attributed as birthing today’s Blockchain industry. Since then, additional Blockchains have been popularized, Ethereum, various Hyperledger project solutions, as well as numerous others including “Blockchain like” solutions such as *GuardTime’s KSI* products

What is Blockchain?

- Blockchain is a system comprised of..
  - Transactions
  - Immutable ledgers
  - Decentralized peers
  - Encryption processes
  - Consensus mechanisms
  - Optional Smart Contracts

- Let’s explore these concepts

Transactions

- **As with enterprise transactions today, Blockchain is a historical archive of decisions and actions taken**
- **Proof of history, provides provenance**

Notable transaction use cases
Land registration – Replacing requirements for research of Deeds (Sweden Land Registration)
Personal Identification – Replacement of Birth/Death certificates, Driver's Licenses, Social Security Cards (Estonia)
Transportation – Bills of Lading, tracking, Certificates of Origin, International Forms (Maersk/IBM)
Banking – Document storage, increased back office efficiencies (UBS, Russia's Sberbank)
Manufacturing – Cradle to grave documentation for any assembly or sub assembly
Food distribution – Providing location, lot, harvest date Supermarkets can pin point problematic food (Walmart)
Audits – Due to the decentralized and immutable nature of Blockchain, audits will fundamentally change.

- **Demo - https://anders.com/blockchain/blockchain.html**

Immutable

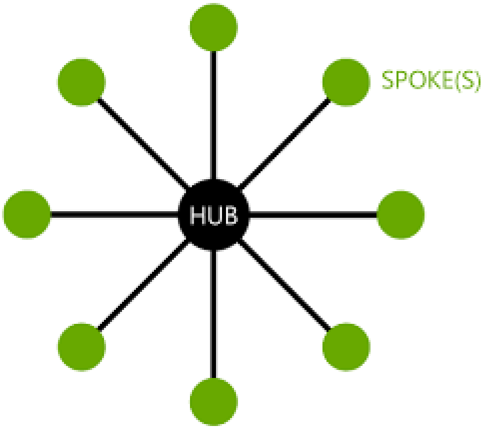
- As with existing databases, Blockchain retains data via transactions
- The difference is that once written to the chain, the blocks can be changed, but it is extremely difficult to do so. Requiring rework on all subsequent blocks and consensus of each.
- The transaction is, immutable, or indelible
- In DBA terms, Blockchains are Write and Read only
- Like a ledger written in ink, an error would be be resolved with another entry

Decentralized Peers

- Rather than the centralized “Hub and Spoke” type of network, Blockchain is a decentralized peer to peer network. Where each NODE has a copy of the ledger.

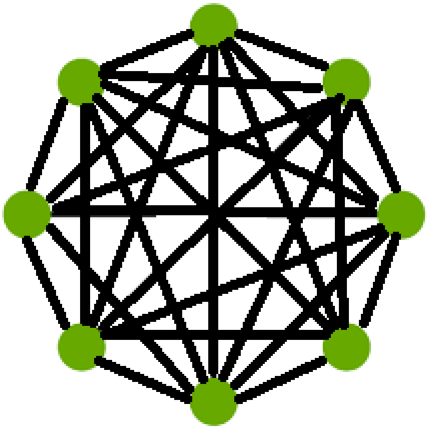
Legacy Network

Centralized DB



Blockchain Network

Distributed Ledgers



Encryption

- Standard encryption practices
- Some Blockchains allow for “BYOE” (Bring Your Own Encryption)
- Only as good as the next hardware innovation
- All blocks are encrypted
- Some Blockchains are public, some are private
  - Public Blockchains are still encrypted, but are viewable to the public, e.g. https://www.blocktrail.com/BTC
  - Private Blockchains employ user rights for visibility, e.g.
    - Customer – Writes and views all data
    - Auditors – View all transactions
    - Supplier A – Writes and views Partner A data
    - Supplier B – Writes and views Partner B data

Consensus

- **Ensures that the next block in a blockchain is the one and only version of the truth**
- **Keeps powerful adversaries from derailing the system and successfully forking the chain**
- **Many Consensus mechanisms, each with pros and cons**

Consensus Mechanism
Proof of Work
Proof of State
Proof of Elapsed Time
Proof of Activity
Proof of Burn
Proof of Capacity
Proof of Importance
And others….

Smart Contracts

- **Computer code**
- **Provides business logic layer prior to block submission**

Blockchain	**Smart Contracts?**	**Language**	
Bitcoin	No		
Ethereum	Yes	Solidity	
Hyperledger	Yes	Various	GoLang, C++, etc, depends
Others	Depends	Depends	

Blockchain Capabilities

A shared ledger technology allowing any participant in the business network to see the system of record (ledger)

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

All parties agree to network verified transaction

Business terms embedded in transaction database & executed with transactions

Blockchain Essentials

1. A business problem to be solved
   - That cannot be solved with more mature technologies
2. An identifiable business network
   - With Participants, Assets and Transactions
3. A need for trust
   - Consensus, Immutability, Finality or Provenance

Negative Indicators, Anti-Patterns

1. Need high performance (millisecond) transactions
2. Small organization (no business network)
3. Looking for a database replacement
4. Looking for a messaging replacement
5. Looking for transaction processing replacement
6. Process and metrics are not clear within the ecosystem
7. Value, velocity and/or variability are not present

Additional Resources

- Bitcoin White Paper – Satoshi Nakamoto
- Blockchain Demo – Anders Brownworth
  - Videos
- Blockchain for Business - An Introduction to Hyperledger Technologies - edX.org
- Ethereum White Paper
- Guardtime – Blockchain *like* official site
- Hyperledger official site - Linux Foundation
- IBM Blockchain for Business – IBM Dev Center
- IBM Blockchain Essentials Course – IBM Dev Center
- IBM Blockchain Foundation Developer – IBM Dev Center

Many more and pages are always changing