Blockchain Demystified

- DLA
- Supplier
- Military Service
- Carrier
- GSA
- Treasury
What you will understand

• A blockchain is
  – a data storage method
  – identical copies are distributed among partners and networked together
  – used to track events in a timestamped list (ledger)
  – once written, it’s unalterable (immutable)

Borrowed from: Paul Baran - Centralized, Decentralized and Distributed networks (1964)
We are on a blockchain of our ancestors

1. DNA is your genetic signature.
2. It is impossible to alter the DNA of your ancestors.
3. Your signature links you back toward your ancestors and forward to your progeny.
Agenda

• When might I use blockchain over other technologies?
• What is a blockchain?
• How would it work for a supply chain network?
• Where might I use it in my operations?
• To learn more, where can I go?
• Demonstration of WaypointIQ – an Ethereum-based application
When do I use a blockchain?

• “If it doesn’t need guaranteed execution, it’s not a blockchain use case”

• What process might need guaranteed execution and/or guaranteed attestation?
  – Ensuring tamperproof digital documentation
  – Authenticating intermodal transportation container seals
  – Managing procurements - requesting a bid and receiving a bid response
  – Tracing the funding and spending of campaign contributions
What:

Concepts you will take away today

• Hashing
• Block
• Blockchain/blockchain network
• Distributed
• Validation and Mining/Consensus
• Trustless
**What:**

A hash is mathematical DNA

<table>
<thead>
<tr>
<th><strong>Clear text</strong></th>
<th><strong>Values from a SHA-256</strong> hash function</th>
</tr>
</thead>
<tbody>
<tr>
<td>“USTRANSCOM”</td>
<td>972bb620a7ff1fda6d719c82bd23a955123e8bbe814a990c1e8a3571f515da1</td>
</tr>
<tr>
<td>“UsTRANSCOM”</td>
<td>df6da099de3040d6d11506cc7d9f05e0ba6b14a182448c23f3c861f890859a9c</td>
</tr>
<tr>
<td>“0”</td>
<td>5feceb66ffc86f38d952786c6d696c79c2dgc39dd4e91b46729d73a27b57e9</td>
</tr>
<tr>
<td>X12 EDI file</td>
<td>d586455736dd2609561047c6b4e52ef281c0dc9a6857f662cb2469207df78100</td>
</tr>
</tbody>
</table>

NIST encourages using SHA-2 and SHA-3 functions

https://www.tools4noobs.com/online_tools/hash/
A block is a collection of individual transactions

- Transactions carry input (data)
- Hashes (digital DNA) make transactions and blocks traceable

What:
Blocks are joined together into a chain
How do you assemble a blockchain?

1. T.O. Pickup Order
2. Carrier Pickup Confirmed
3. Accounting Credit

- Validate the new transaction(s)
- Solve for the new block
- Get consensus from the network
- Commit the new block to the chain

Time
How many mining attempts to solve for the digital DNA of a Bitcoin block?

The October 2019 Bitcoin network produced a hash rate* of:

90,000,000,000,000,000,000 hashes per second, or 90 quintillion** h/s.

54 sextillion*** hashes are accomplished in 10 minutes to solve for the digital DNA of a bitcoin block

... a white buffalo occurs 1 time out of every 10 million...

** six groups of (3) zeros
*** seven groups of (3) zeros
Trustless vs. trust

Trustless – a concept from cryptocurrency. By using the bitcoin network to exchange cryptocurrency, there is no longer the need for a trusted third-party (like a bank) middle-man to transfer currency among transacting parties. “You may trade money in a trustless environment”

Trust – You can trust the blockchain to ensure that its data is authentic, valid, and unalterable (immutable).
How could a blockchain trace my operations?

• For the following example, let's assume:
  – Unanimous agreement to adopt the same blockchain
  – All information will fit into the blockchain
  – We’ve resolved issues like security, privacy, access privileges, etc.
How:
Watching supply chain transactions
How:
Watching supply chain transactions
How:
Watching supply chain transactions
How:

Watching supply chain transactions
Where might I use it in my operations?

- **Physical Assets**
  - Authenticate the origin of high-value components
  - Record the various states of an asset’s lifecycle

- **Digital Assets**
  - Record and preserve a cryptocurrency ledger
  - Fingerprint technical data packages (TDPs) prior to distribution
  - Record acquisition lifecycle artifacts
  - Provide a transparent record of political campaign contributions
Demonstration Concept of operations – Tracking the state of Assets

- Register/Authenticate Assets
- Ship Assets
- Receive Assets
- Quarantine Assets

Additional Asset States
- Create
- Consume
- Assemble
- Disassemble
- Demilitarize

System Boundary
Learning more – a reading list

White Papers & Books

• **Blockchain**, Swan, O’Reilly Media, 2015
• **Hashcash - A Denial of Service Counter-Measure**, Adam Back. 2002
• **Bitcoin: A Peer-to-Peer Electronic Cash System**, Satoshi Nakamoto. 2008
• **Mastering Bitcoin**, Andreas Antonopoulos. O’Reilly. 2015
• **A Next-Generation Smart Contract and Decentralized Application Platform**, Vitalik Buterin. 2014
• **A Treatise on Altcoins**, Andrew Poelstra. 2016
• **Mimblewimble**, Andrew Poelstra. 2016
• **A Lightweight Blockchain Consensus Protocol**, Keir Finlow-Bates
• **Proof of Activity: Extending Bitcoin’s Proof of Work via Proof of Stake**, Iddo Bentov, Charles Lee, Alex Mazrahi, Meni Rosenfeld.
• **Blockchain: The Solution for Transparency in Product Supply Chains**, Provenance. 2015

Research Reports

• **Hype Cycle for Chief Supply Chain Officers**, C. Dwight Klappich. Gartner Report 2016
Learning:

Some of my favorites

- **The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order** by Paul Vigna and Michael J. Casey
- **YouTube’s CuriousInventor: How Bitcoin Works Under the Hood**
- **https://www.ccn.com/blockchain-allows-sneaker-manufacturer-prevent-counterfeiting/**
- **Code to Inspire (CTI) – Building Afghanistan 2.0**
- “so called immutability…It is the result of the ongoing interplay of incredibly intricate mathematics and economic incentives.”
Thank you

Gus Creedon
Sr. Consultant, Systems Engineer
INCOSE ASEP – Associate Systems Engineering Professional™
Certified Scrum Product Owner® Professional
ITIL® Foundation

LMI Digital Services
7940 Jones Branch Drive, Tysons, VA 22102
gcreedon@lmi.org

LMI