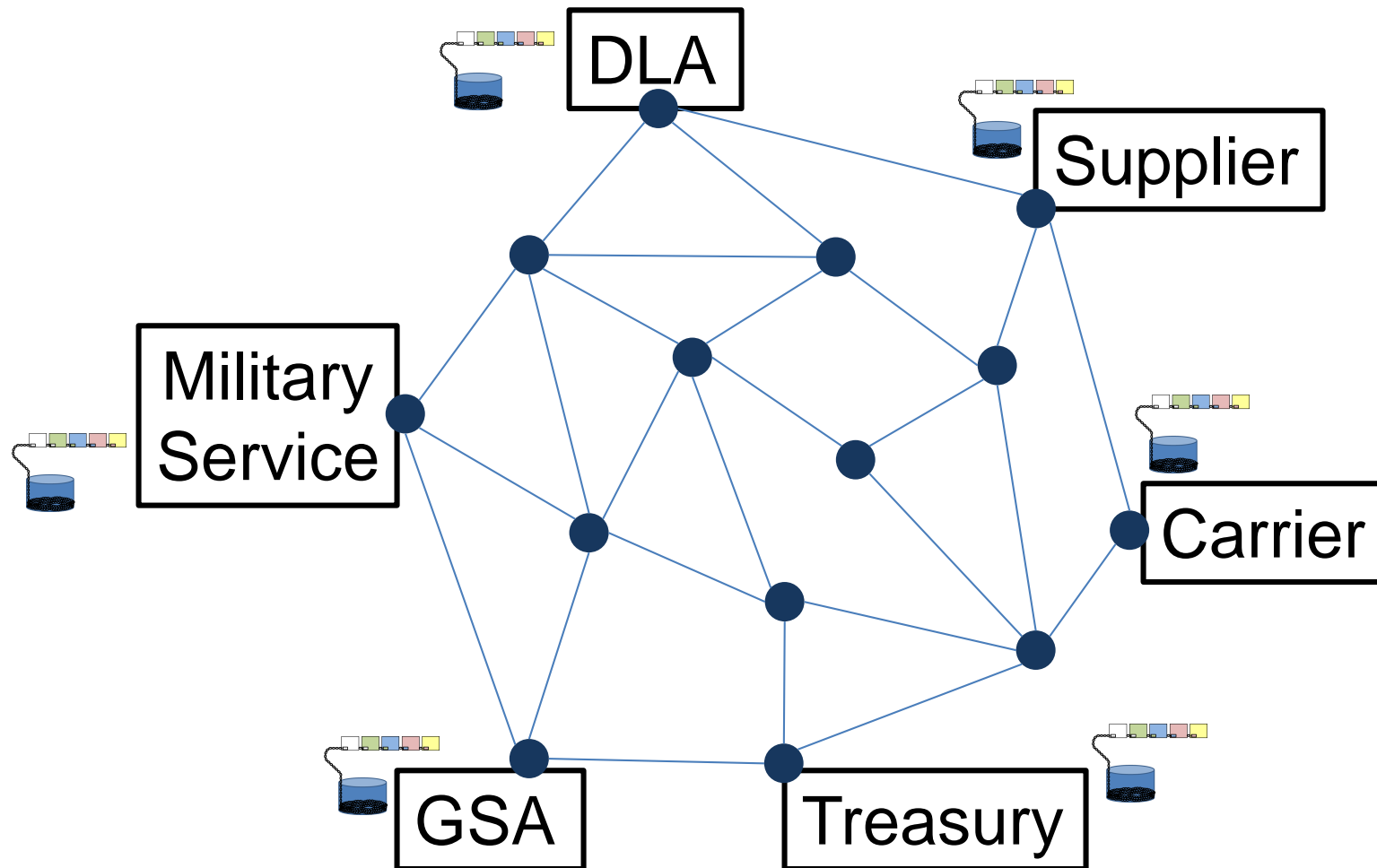
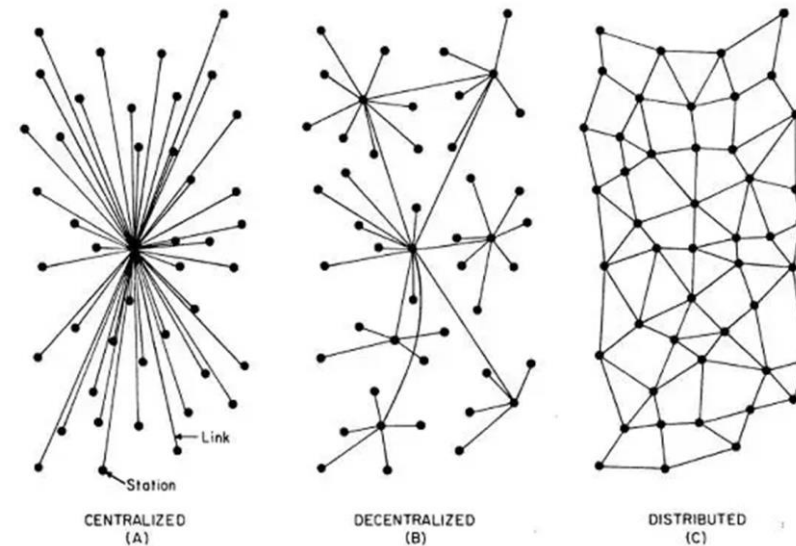


Blockchain Demystified



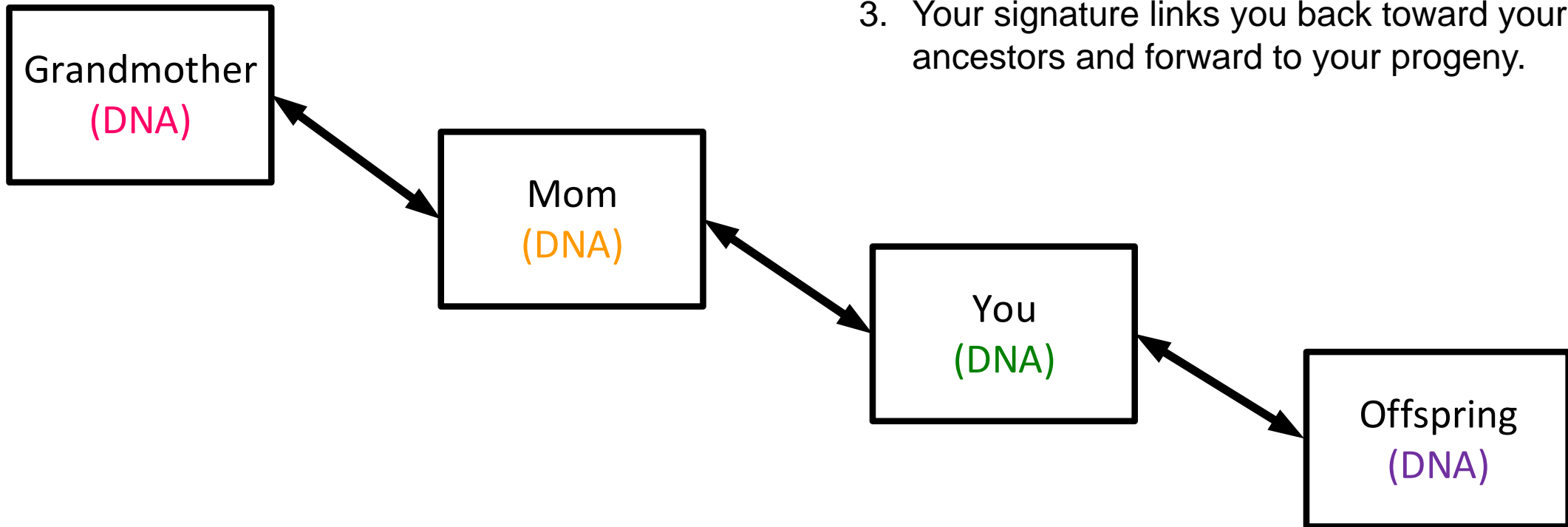
What you will understand

- 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)



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”
Diedrich, Henning. *ethereum - blockchains, digital assets, smart contracts, decentralized autonomous organizations*. Wildfire Publishing, 2016.
- 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

hash function + “string of characters” = hash value

Clear text**Values from a SHA-256** hash function**

“USTRANSCOM”	972bb620a7ff1fda6d719c82bd23a955123e8bbef814a990c1e8a3571f515da1
“UsTRANSCOM”	df6da099de3040d6d11506cc7d9f05e0ba6b14a182448c23f3c861f890859a9c
“0”	5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9
X12 EDI file	d586455736dd2609561047c6b4e52ef281c0dc9a6857f662cb2469207df78100

NIST encourages using SHA-2 and SHA-3 functions

What:

A block is a collection of individual transactions

Block header

Number	PreviousHash	DataHash
--------	--------------	----------

Transaction 1

Tx-1 Type	Version	Timestamp	Channel Id	Txid	Epoch	PayloadVisibility
Chaincode Path (deploy tx)		Chaincode Name (invoke tx)		Chaincode Version		
Transaction's Creator Identity (certificate, public key) - Client						Signature
Chaincode Type	Input (chaincode function and arguments)				Timeout	
Start Key	End Key	List of <Key, Version> read		Merkel Tree Query Summary		

GBL - Cherry Point

Transaction 2

Tx-1 Type	Version	Timestamp	Channel Id	Txid	Epoch	PayloadVisibility
Chaincode Path (deploy tx)		Chaincode Name (invoke tx)		Chaincode Version		
Transaction's Creator Identity (certificate, public key) - Client						Signature
Chaincode Type	Input (chaincode function and arguments)				Timeout	
Start Key	End Key	List of <Key, Version> read		Merkel Tree Query Summary		

Trans-shipped - Rotterdam

Transaction 3

Tx-1 Type	Version	Timestamp	Channel Id	Txid	Epoch	PayloadVisibility
Chaincode Path (deploy tx)		Chaincode Name (invoke tx)		Chaincode Version		
Transaction's Creator Identity (certificate, public key) - Client						Signature
Chaincode Type	Input (chaincode function and arguments)				Timeout	
Start Key	End Key	List of <Key, Version> read		Merkel Tree Query Summary		

Manifest - Dover



Transaction n

Tx-1 Type	Version	Timestamp	Channel Id	Txid	Epoch	PayloadVisibility
Chaincode Path (deploy tx)		Chaincode Name (invoke tx)		Chaincode Version		
Transaction's Creator Identity (certificate, public key) - Client						Signature
Chaincode Type	Input (chaincode function and arguments)				Timeout	
Start Key	End Key	List of <Key, Version> read		Merkel Tree Query Summary		

Delivery - Osan

Block footer

Last offset persisted: Kafka	Creator Identity (certificate, public key)	Signature
------------------------------	--	-----------

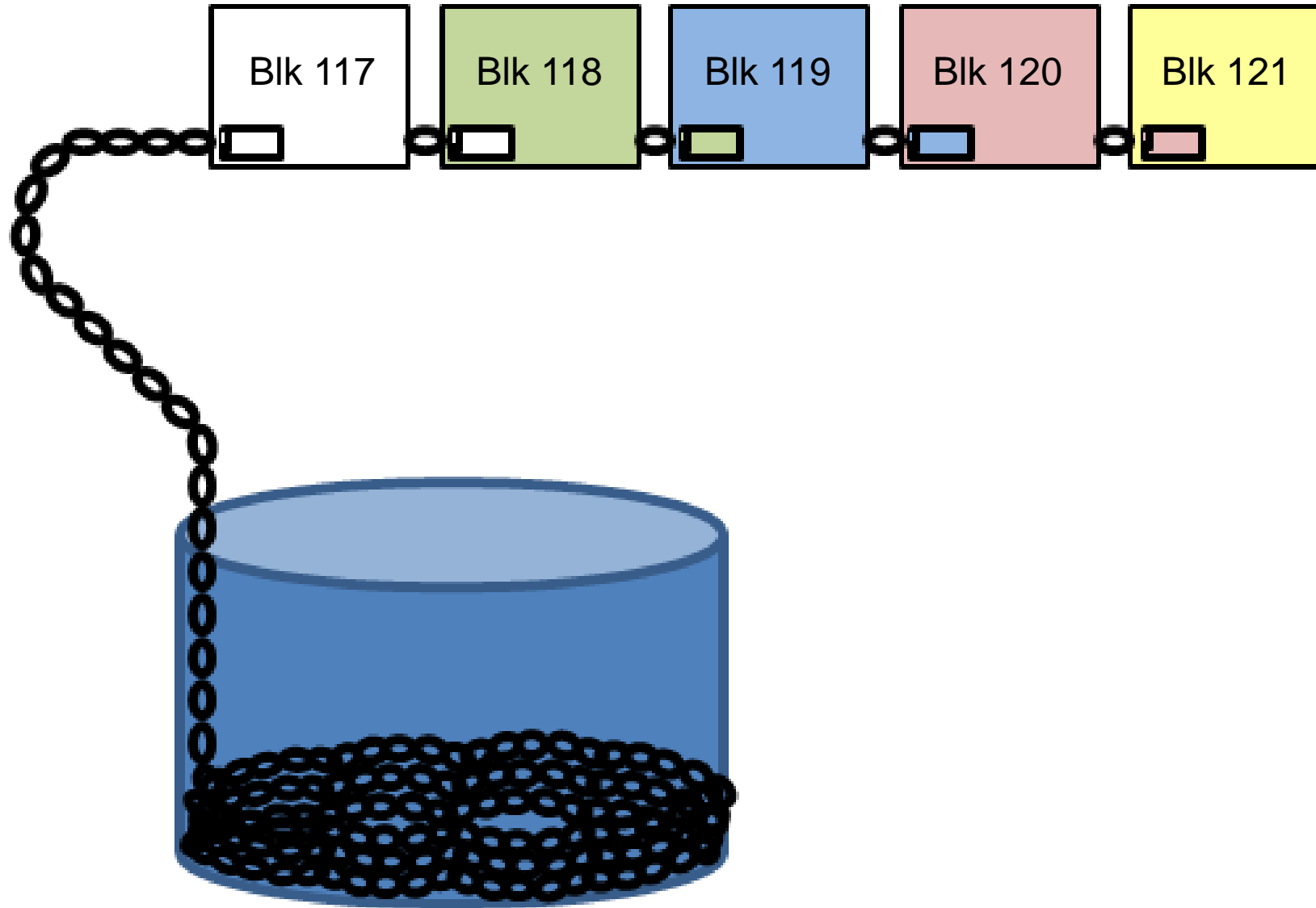
- Transactions carry input (data)
- Hashes (digital DNA) make transactions and blocks traceable

Structure diagram credit:

<https://blockchain-fabric.blogspot.com/2017/04/hyperledger-fabric-v10-block-structure.html>

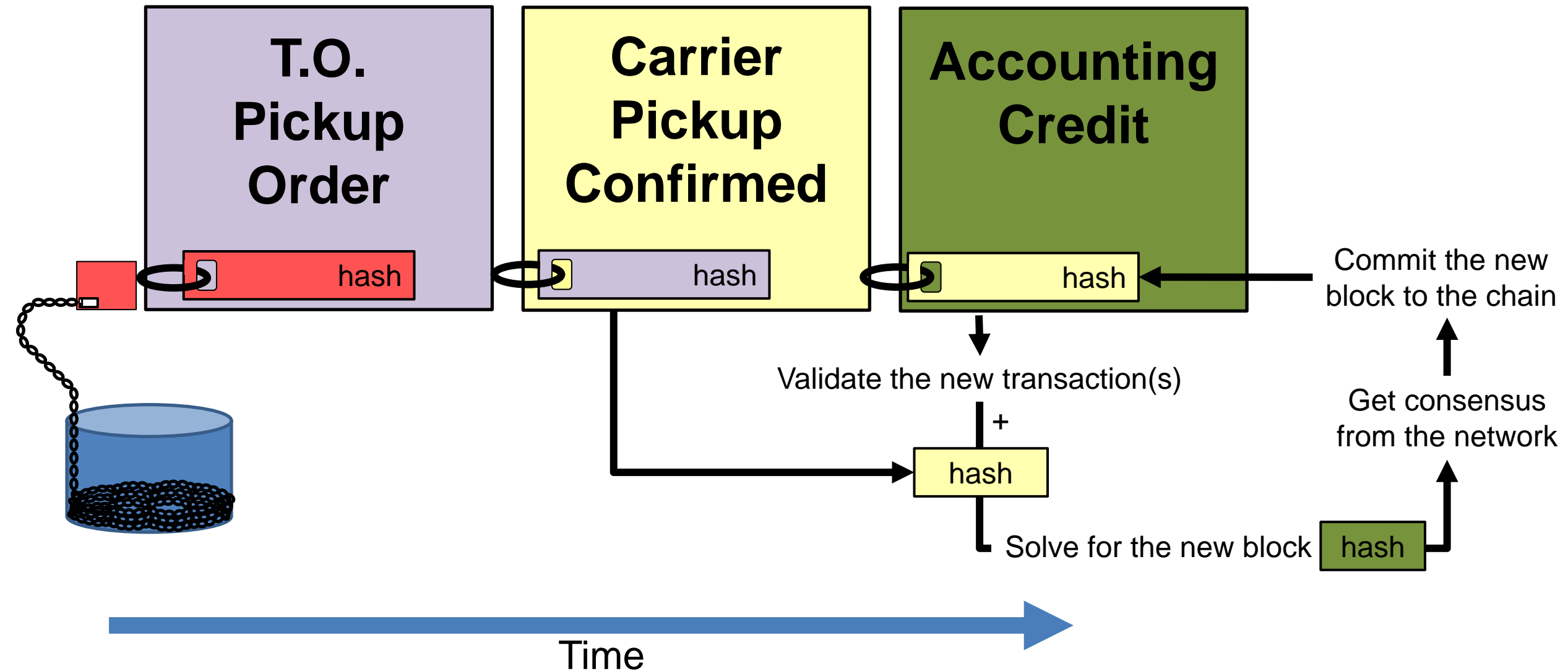
What:

Blocks are joined together into a chain



What:

How do you assemble a blockchain?



What:

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...

*<https://www.blockchain.com/en/charts/hash-rate>

** 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”

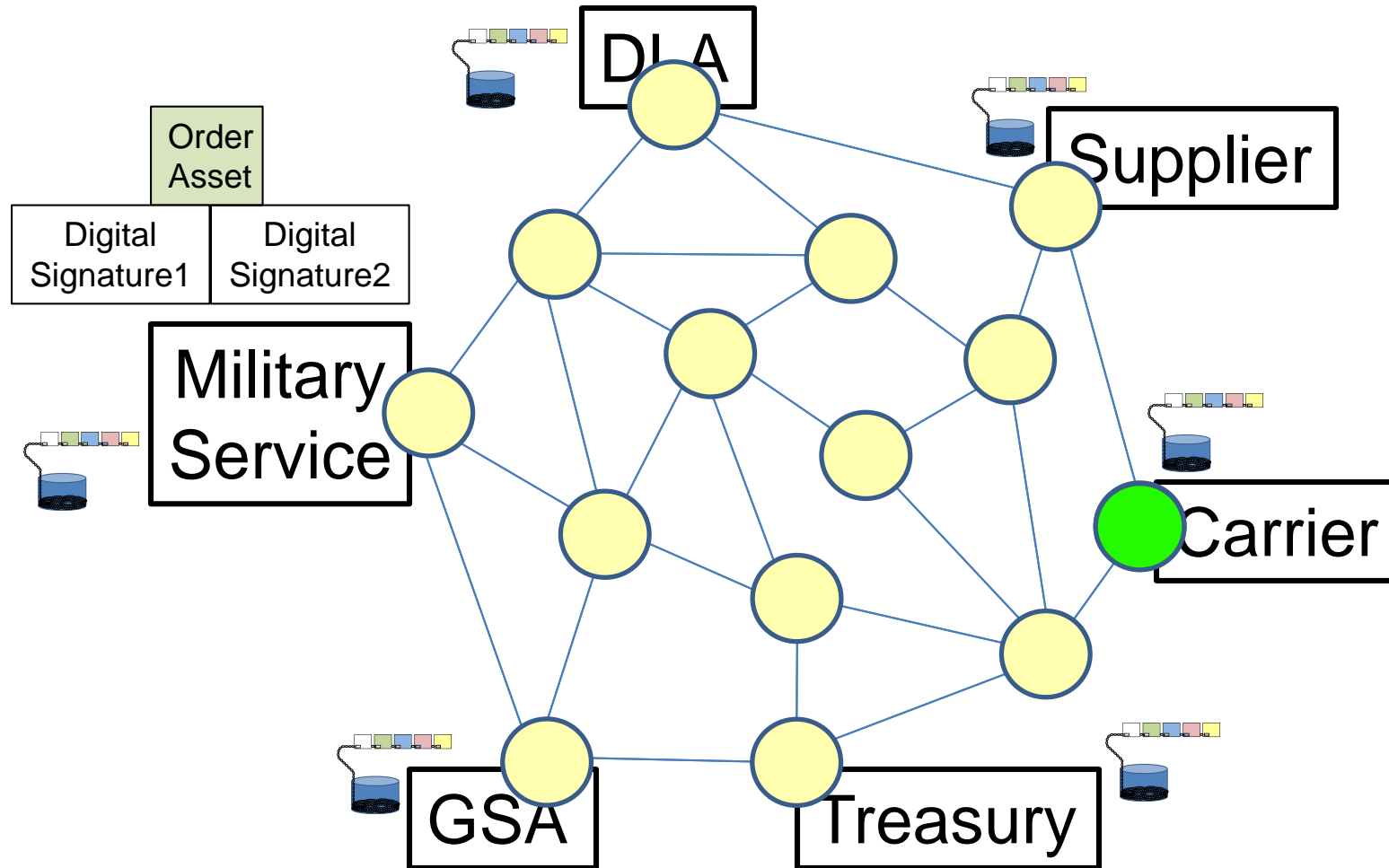
Trust – You can trust the blockchain to ensure that its data is authentic, valid, and unalterable (immutable).

How could a blockchain trace my operations?

- For the following example, lets 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.

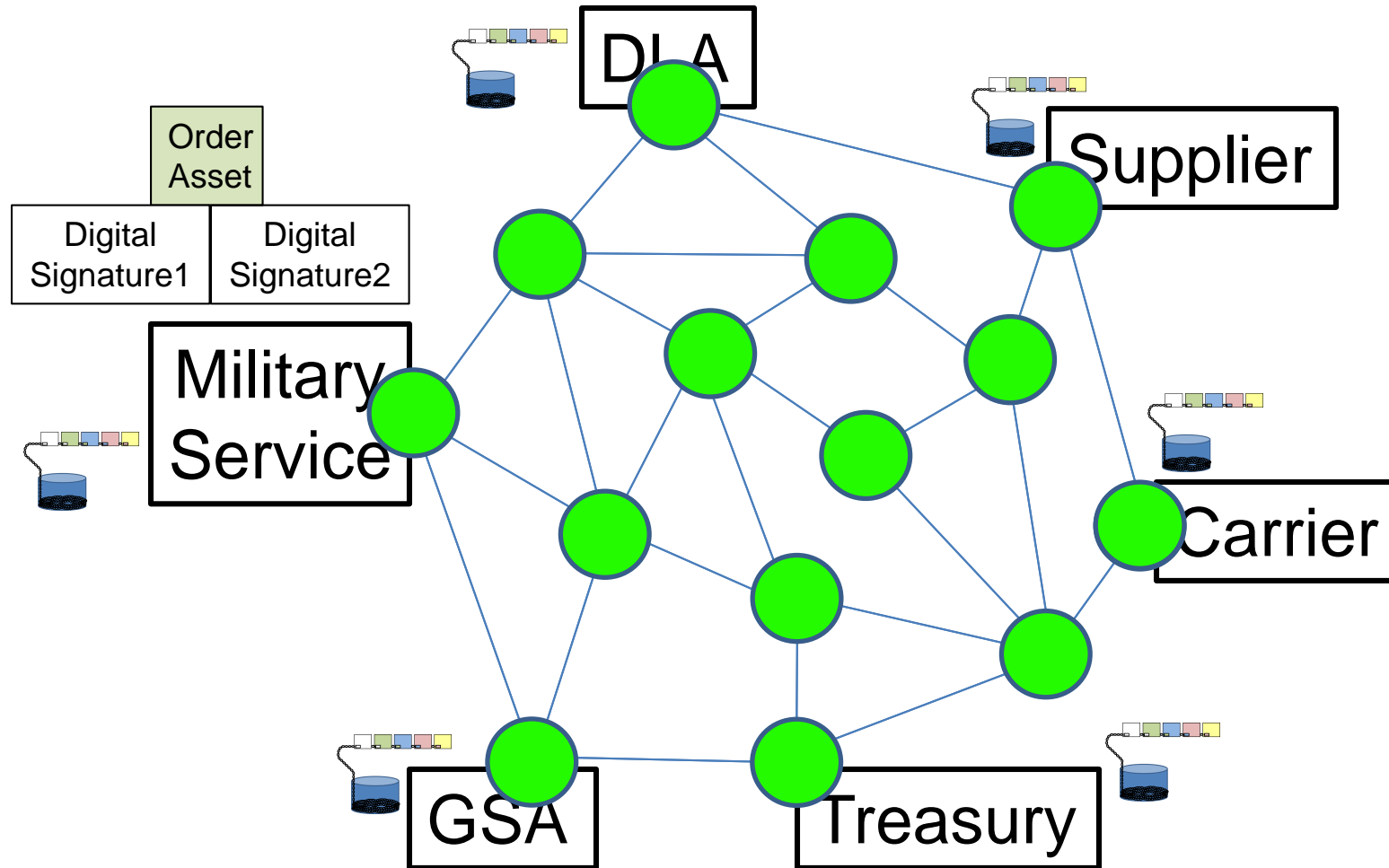
How:

Watching supply chain transactions



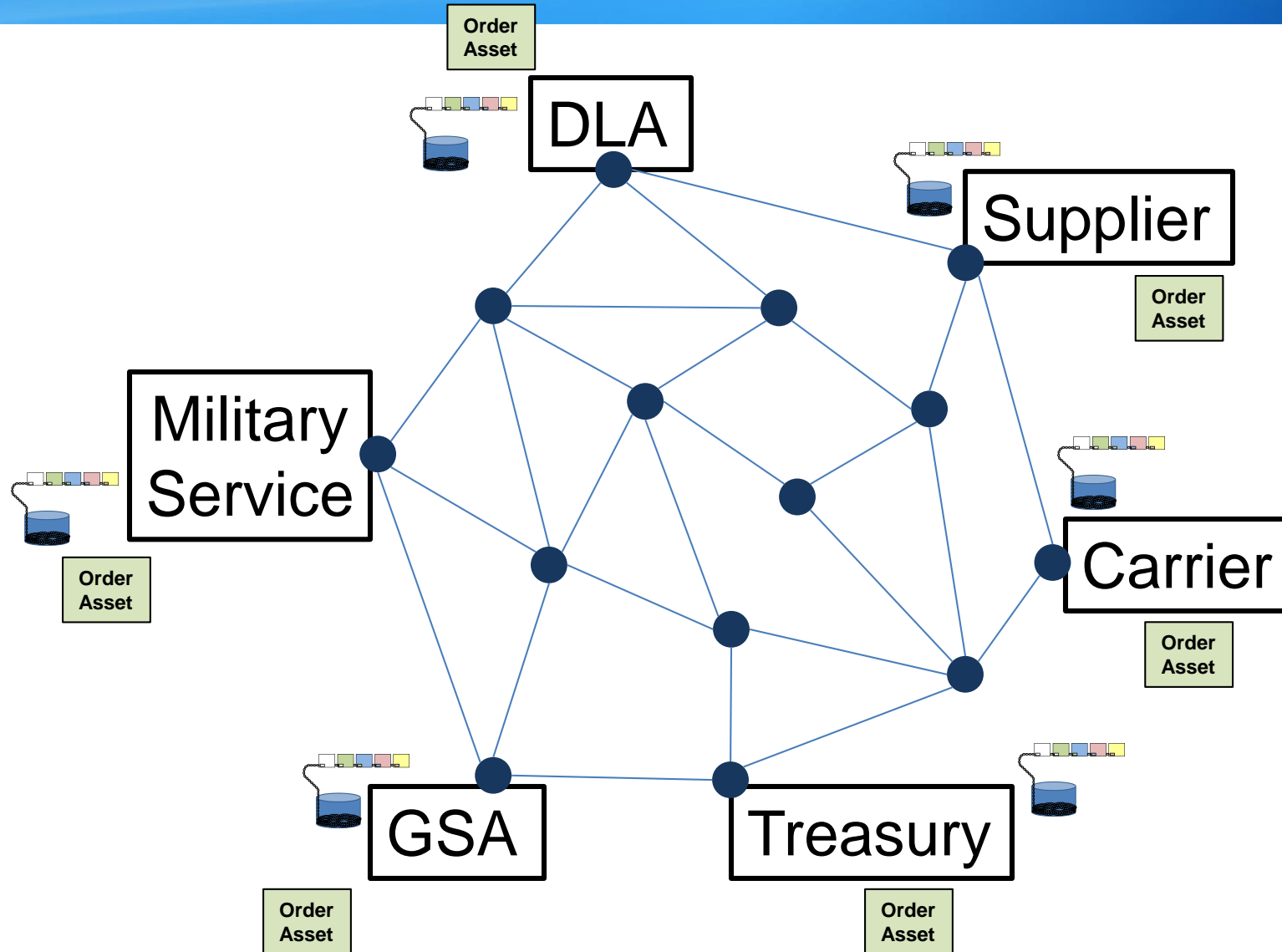
How:

Watching supply chain transactions



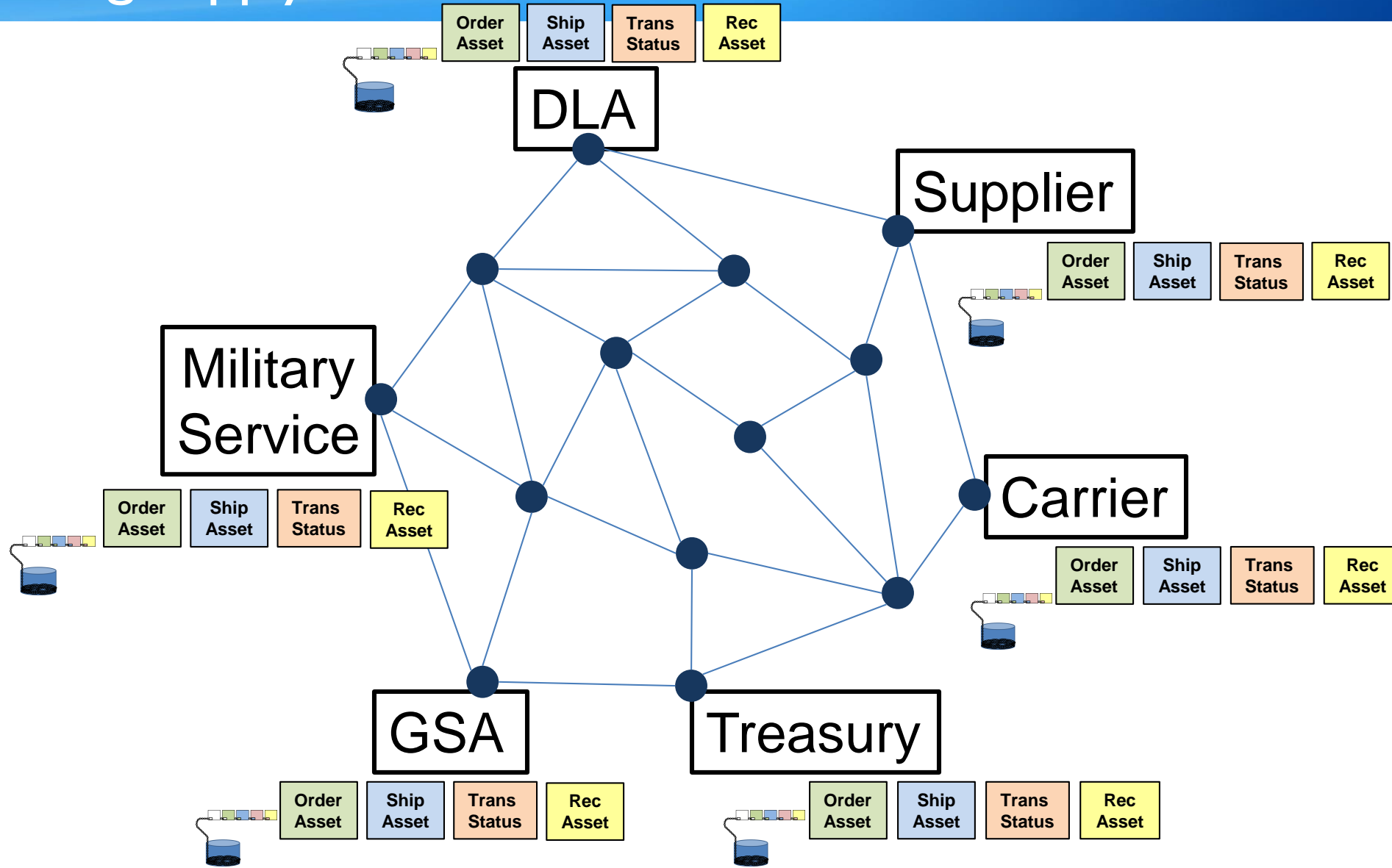
How:

Watching supply chain transactions



How:

Watching supply chain transactions



Where might I use it in my operations?

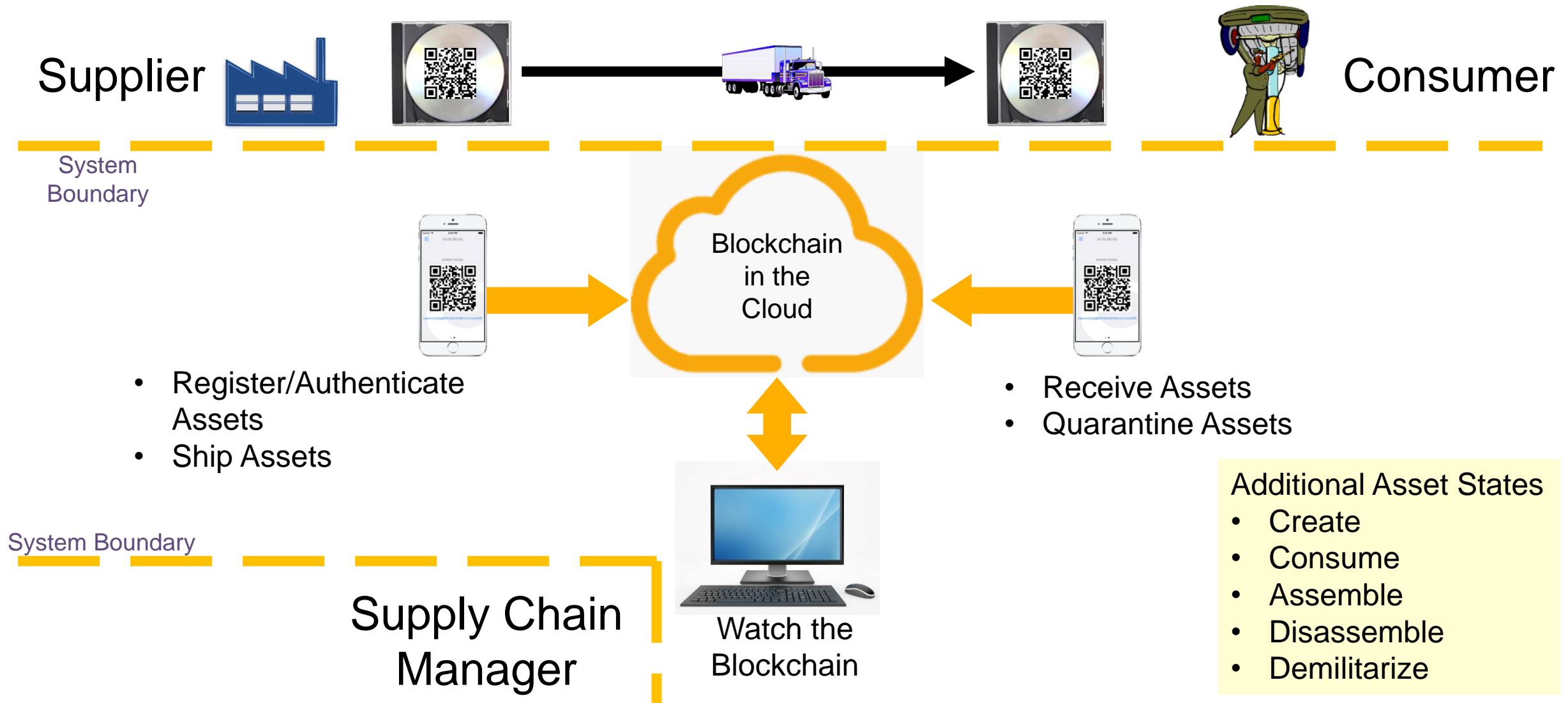
- **Physical Assets**

- 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



Learning more – a reading list

White Papers & Books

- **THE AGE OF CRYPTO CURRENCY, HOW BITCOIN AND BLOCKCHAIN ARE CHALLENGING THE GLOBAL ECONOMIC ORDER**, Paul Vigna and Michael Casey, St. Martin's Press, 2015.
- **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
- **Introducing Project Bletchley**. Marley Gray. Microsoft. 2016
- **Architecture of the Hyperledger Blockchain Fabric**. Christian Cachin. IBM Research. 2016
- **Ethereum, - blockchains, digital assets, smart contracts, decentralized autonomous organizations**. Henning Diedrich, Wildfire Publishing, 2016.
- **A Treatise on Altcoins**. Andrew Poelstra. 2016
- **Mimblewimble**. Andrew Poelstra. 2016
- **A Lightweight Blockchain Consensus Protocol**. Keir Finlow-Bates
- **The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments**. Joseph Poon and Thaddeus Dryja. 2016
- **Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake**. Iddo Bentov, Charles Lee, Alex Mizrahi, Meni Rosenfeld.
- **The Stellar Consensus Protocol**. David Mazieres. Stellar Development Foundation. 2016
- **Ethereum: A Secure Decentralized Generalized Transaction Ledger**. Gavin Wood. Ethereum.
- **Ethereum 2.0 Mauve Paper**. Vitalik Buterin. Ethereum. 2016
- **The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication**. Marko Vukolic. IBM Hyperledger.
- **Blockchain Technology and Cryptocurrencies: Opportunities for Postal Financial Services**. Christian Jaag and Christian Bach. Swiss Economics. 2016.
- **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
- **Building Trust In Government**. IBM Institute for Business Value Executive Report. 2017.
- **Evaluation Forms for Blockchain-Based System**. Information Economy Division of Japan's Ministry of Economy, Trade, and Industry (METI). 2017.
- **State of Blockchain – 2016 Year in Review**. CoinDesk. 2016
- **Innovation Insight for Blockchain Security**. Jonathan Care and David Mahdi. Gartner Report 2016.
- **Distributed Ledger Technology: beyond block chain**. UK Government Chief Scientific Adviser Report. 2016.
- **How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?** Brett Scott. United Nations Research Institute for Social Development (UNRISD) report. 2016.
- **Understanding Ethereum**. CoinDesk Report. 2016.
- **Editing the Uneditable Blockchain**. Richard Lumb. Accenture Report. 2016.
- **Blockchain Applications in the Public Sector**. Alexander Shelkovich. Deloitte Report. 2016.

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
 - <https://www.codetoinspire.org/bitcoins-and-beyond-creating-a-financial-future-for-afghanistan-women/>
- “so called immutability...It is the result of the ongoing interplay of incredibly intricate mathematics and economic incentives.”
 - <https://www.coindesk.com/programming-blockchain-will-change-see-bitcoin/>

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



