Blockchain: Building Consensus and Trust across the Space Sector

Karen L. Jones
Center for Space Policy & Strategy
The Aerospace Corporation

Karen.l.jones@aero.org

April 8, 2019

Why Should I Care?

"Blockchain technologies have the power to disrupt many industries. To avoid missed opportunities and undesirable surprises, organizations should start investigating whether or not a blockchain can help them."

-- National Institute of Standards and Technology; U.S. Department of Commerce; "Blockchain Technology Overview"; January 2018

Purpose

- Understand how blockchain and distributed ledger technologies (DLT) are evolving across various applications.
- Highlight some use case scenarios to understand relevance to space sector challenges.

Inclusion or exclusion of use cases does not validate or invalidate any application. We welcome comments and insight to shape our understanding of blockchain and its relevance in the space sector.

Blockchain is not always appropriate – it depends upon the application scenario.

When does blockchain make sense?

- ***Trust*** - Multiple mutually mistrusting entities want to interact
- ***State*** - Need to maintain and change the state of a system as new transactions occur (e.g. database with transactional data)
- ***Distribution*** - Desire to "disintermediate" the existing centralized third party to harness greater efficiency or value OR unwilling to agree on an online trusted third party.

When does blockchain not make sense?

- There is no stored data in a database
- Target application currently uses trusted entities which interact well
- A trusted third party functions well and efficiently as verifiers for ***state*** transitions (e.g. centralized status quo works well).

Whether or not blockchain is appropriate depends upon trust assumptions, application requirements, involved parties and operational parameters (e.g. capacity, latency, access, etc…)

Treacherous Lexicon…

If you are confused…. you should be…

- Blockchain related vocabulary has been aptly described as:
  - *Muddled*
  - *Contested*
  - *Fluid*
- Inconsistent and poorly understood lexicon can lead to:
  - *Inappropriate adoption*
  - *Ongoing confusion*
  - *Project failure*
  - *Flawed decisions*

Private Key

BOUNTY

Hashgraph

Cryptocurrency Fork

DLT

dAPPS

Airdrop

Cryptocurrency

- ***Token***
- ***Utility Token***
- ***Altcoin***
- ***Security Token***
- ***Penny Crypto***

HyperLedger

Whales

FUD

PROOF OF WORK VS PROOF OF STAKE

A common taxonomy and lexicon will increase confidence and understanding.

Distributed Ledger Technology (DLT)

Blockchain is a subset or type of DLT….

Key DLT elements:

- **Distributed database** – Every node on the network maintains its own copy of the transaction data and other data on the "block", and updates with each new transaction.
- **Peer-to-peer transmission** - no central point of storage, such as a server. Information is being recorded and interchanged between participants (or nodes) on the network.
- **Trust** – A new record's authenticity can be verified by the entire community.
- **Transparency** – Transaction history available to those with ledger permissions.
- **Immutable records** - Any one person is prevented from altering the legitimacy of the information.
- **Embedded logic** – enables process automation, algorithms and rules automatically trigger transactions between nodes.

Blockchain is a type or subset of DLT which includes cryptographically linked "blocks" (e.g. list of transactions), and a "chain" where each block is timestamped and placed in chronological order.

Blockchain technology and how it works

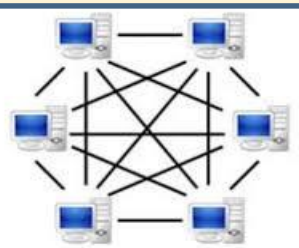
Blockchain involves a ledger or record of digital transactions. The distributed database maintains a growing list of data records or "blocks"" that are cryptographically linked on a "chain".

Start: Person adds funds to a digital wallet (e.g. Ethereum or Bitcoin) and uses an encrypted digital signature

Private Key

Broadcast: Requested transaction is shared through a peer-to-peer (P2P) networking using a public key.

Public Key

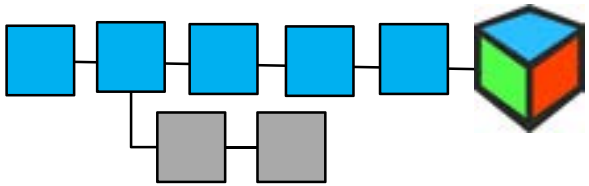


P2P-network

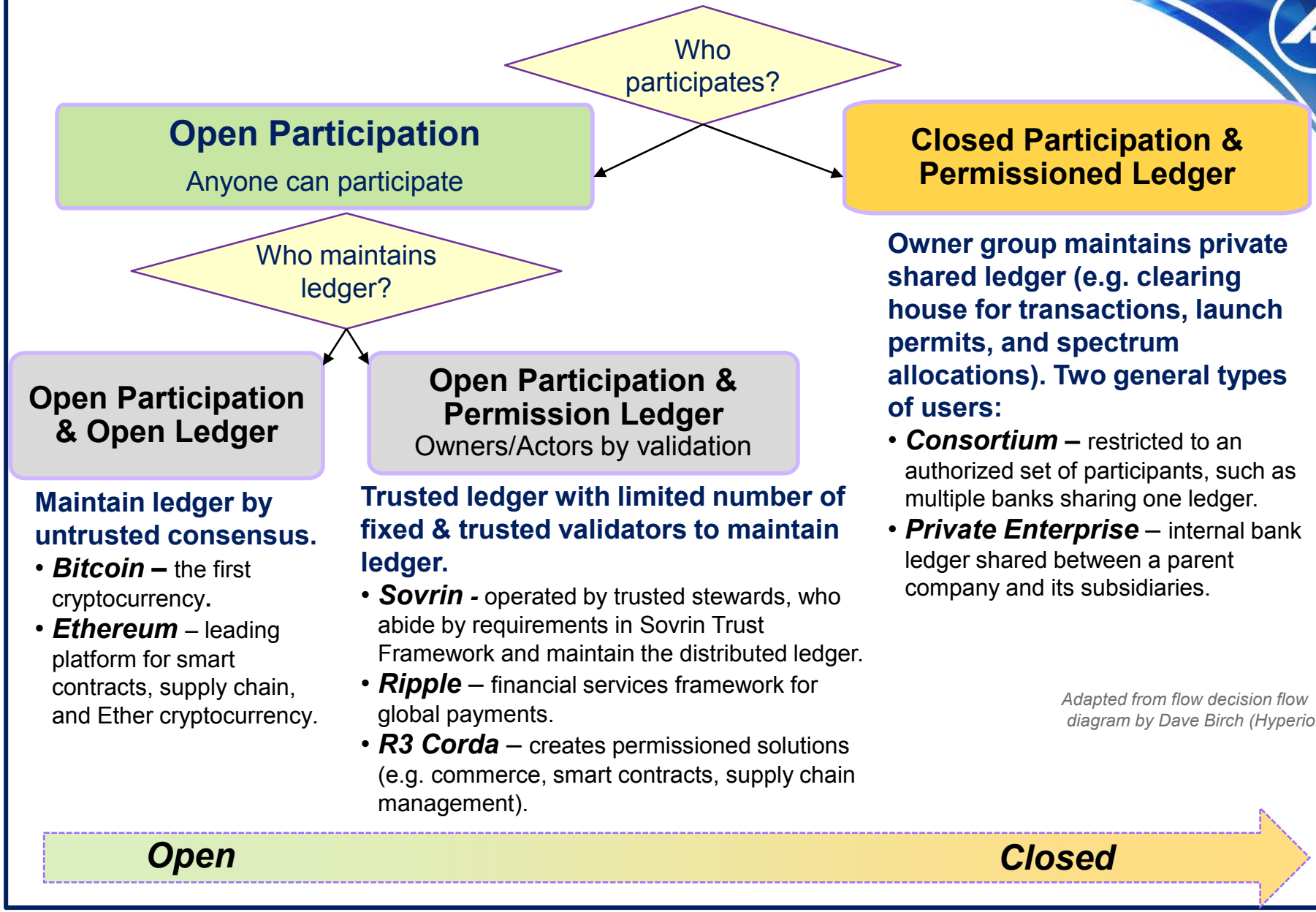
Validation: Computers or "nodes" in the network verify & validate transaction

Add Block to Chain:
Post verification, block is added to the chain in a way that is permanent and unalterable

- Each block contains transaction content and a header, including:
  - information about the block
  - reference to the previous block
  - unique set of random numbers or "*hash*"
- Blocks of records in the same timestamp are added as branches to the block.

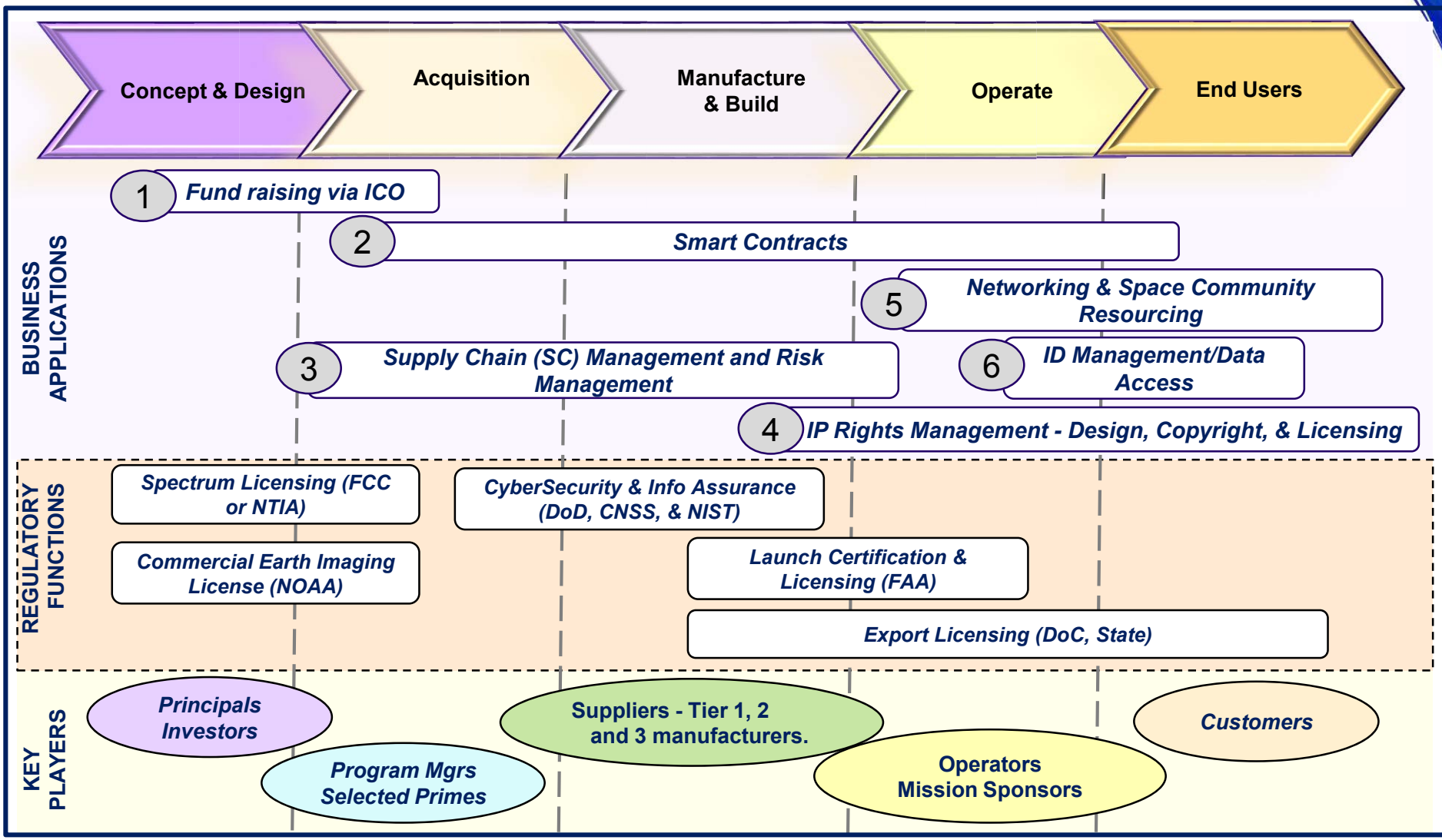


Transaction Complete


Who participates?
Open Participation
Anyone can participate
Closed Participation & Permissioned Ledger
Who maintains ledger?
Open Participation & Open Ledger
Open Participation & Permission Ledger
Owners/Actors by validation
Maintain ledger by untrusted consensus.
• Bitcoin – the first cryptocurrency.
• Ethereum – leading platform for smart contracts, supply chain, and Ether cryptocurrency.
Trusted ledger with limited number of fixed & trusted validators to maintain ledger.
• Sovrin - operated by trusted stewards, who abide by requirements in Sovrin Trust Framework and maintain the distributed ledger.
• Ripple – financial services framework for global payments.
• R3 Corda – creates permissioned solutions (e.g. commerce, smart contracts, supply chain management).
Owner group maintains private shared ledger (e.g. clearing house for transactions, launch permits, and spectrum allocations). Two general types of users:
• Consortium – restricted to an authorized set of participants, such as multiple banks sharing one ledger.
• Private Enterprise – internal bank ledger shared between a parent company and its subsidiaries.
Adapted from flow decision flow diagram by Dave Birch (Hyperion)
Open
Closed

Blockchain in the Space Sector Value Chain

Potential opportunities for consensus based protocols



Space Sector Examples

Lifecycle maturity phase for space and other industries.

Application	Example	Phase (R&D, Demo, Growth, Mature)
1 - Financing New Ventures	Fund raising via Initial Coin Offerings (ICOs) *Space Decentral*	**Non-space – Growth/Mature** **Space - Demo**
2 - Smart Contracts	European Space Agency – *Space 4.0*, and practical administrative DLT applications.	**Non-space - Growth** **Space - Demo**
3 - Supply Chain Management	Applications could include efficient cross enterprise inventory management, tracking of faulty or counterfeit parts.	**Non-space - Growth** **Space – R&D**
4 - IP Management	Applications could include managing licenses for image and data providers.	**Non-space – Demo** **Space – R&D**
5 - Networking & Space Community Resourcing	- NASA - *Resilient Networking and Computing Paradigm* - NASA – *Sensor Web* - Blockchain Nodes – *SpaceChain* - Open Source Networking - *EtherSat*	**Non-space - Growth** **Space - Demo**
6 - ID Management	Non-space sector maturing rapidly. ID applications include - Sovrin, uPort, OneName and ShoCard. Space sector will most like follow and adopt commercial ID management solutions over time.	**Non-space - Growth** **Space - Demo**

Space industry DLT implementations are embryonic (R&D and demo phase). The finance and gaming industry are pathfinders. Other early adopters include insurance, real estate, music, legal and healthcare.

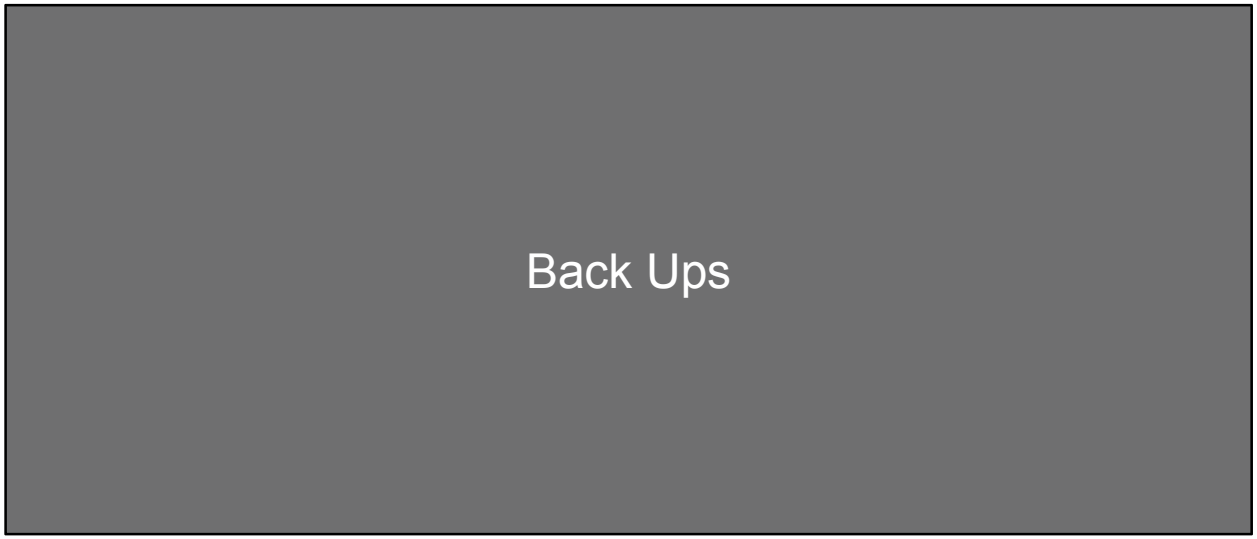
Conclusion:

DLT may endure a prolonged gestation period in the space sector.

- *DLT requires a **paradigm shift** to:*
  - *introduce new forms of governance for making rule-governed economic orders -- rather than an institutional centric order.*
  - *compete with firms, markets and economies as institutional alternatives for coordinating economic actions of groups of people.*
- Most space sector DLT functions require the ***cooperation*** of commercial and government space players.
  - ***Open DLT** - ICO venture financing, directly involve the public*
  - ***Closed/Permissioned** – involving commercial and govt. space players – examples: smart contracts, supply chain management, IP rights, networking, and ID management.*
- Watch for local demos advancing towards enterprise wide models, eventually some may transition to industry wide models.

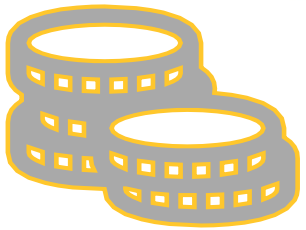
Foundational technologies, such as DLT, require years even decades to take hold.

Back Up Slides



Financing New Ventures

Initial Coin Offerings – Disrupting the Disrupter



- Fundraising in the form of cryptocurrency tokens
  - *now competes with crowdsourcing and can introduce greater efficiencies.*
  - *Example - Ethereum "Acorn" – seeks to create an open community and marketplace for crowdfunding. Platform includes a peer to peer smart contract based upon governance structure and service – overcomes geographic, political and economic borders.*

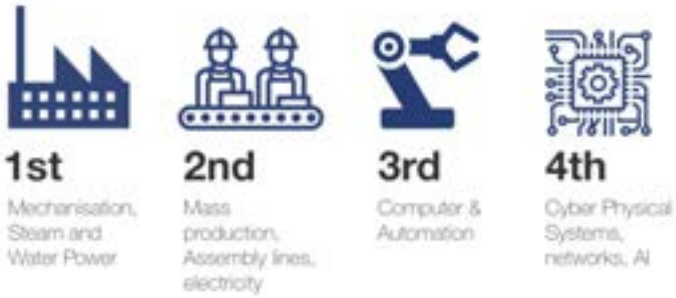
- ***Example - Space Decentral***
  - *"Decentralized Autonomous Organization" uses blockchain to "reinvigorate the push for space exploration with the public in control".*
  - *Design space missions collaboratively and share research for peer review*
  - *crowdsource citizen science efforts*
  - *crowdfund projects that lack national budgets.*
  - *plans to use blockchain technology to coordinate workflows and business logic and use self-executing smart contracts and tokens.*
  - *Current Phase: community of interest and a draft white paper*

ICOs typically are public facing DLTs and are often the most "open" type of DLT application.

Smart Contracts

Self-executing contracts

- **Smart Contracts**
  - *digitally facilitate, verify, or enforce the negotiation or performance of a contract.*
  - *rely on embedded logic which can automatically trigger events when certain conditions are met.*
- **Example** - ***European Space Agency – Space 4.0***
  - *complex and automated interactions between governments, private sector, society and politics.*
  - *accurate payments, procurement, supplier agreements, and automated smart contracts.*
  - *ESA envisions a sustainable space sector closely connected with the fabric of society and economy – and DLT could become an enabling technology to support this vision*



Self-executing contracts could address the complexity of stakeholders and their obligations -- from launch to orbit.

Supply Chain Management

A forensic audit trail and single source of truth

- Stakeholders do not have an adequate view of their supply chain. They have various data silos and there is not much incentive to share data.
- Yet end customers, including space sector participants, demand greater levels of transparency to:
  - *Detect cyber threats*
  - *Manage accurate inventory levels*
  - *Respond to product recalls in a timely manner*
  - *Detect faulty and counterfeit parts*
- **DoD supply chain risk management policy** - requires DoD organizations to identify critical information and communications technology components, purchase those components from trusted suppliers, and test and evaluate critical components for malicious threats.

As the space sector expands it us of off-the-shelf (OTS) parts, DLT applications for supply chain management could become increasingly critical.

IP Management

For Copyrights, Design, Data Management and User Licenses

- DLT can be applied as a registry of IP rights
  - *Potential to support inventors and creators*
  - *Establish a decentralized registry and digital trail for innovation*
  - *Could replace the long and tedious process for idea protection and patents*
  - *Could help companies and inventors quickly discover prior art, and better help articulate ideas and invention novelty*
- Potential space applications could include tracking and protection of:
  - *space imaging data rights*
  - *analytics and software*
  - *other digital rights*

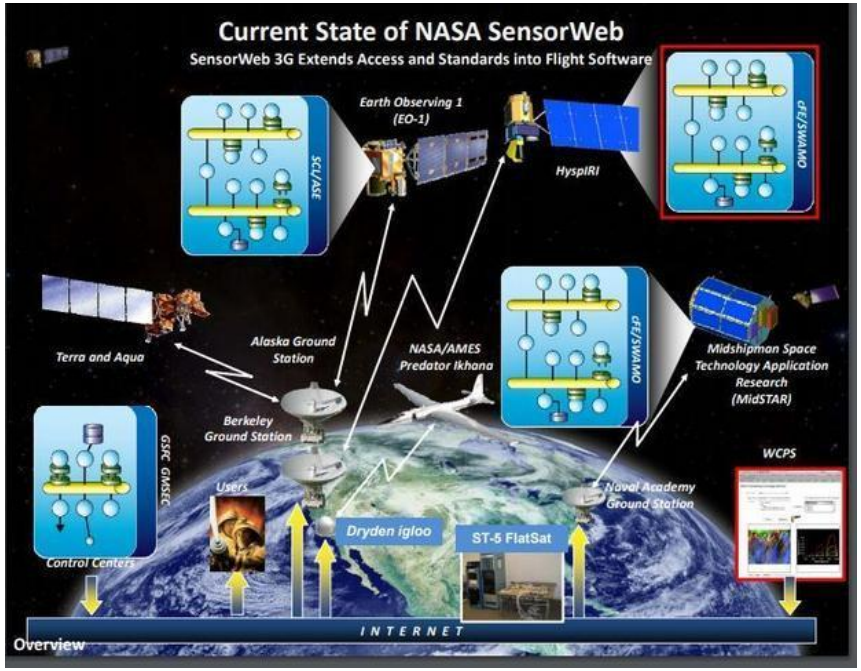
- ***Blockchain technology will have the potential to completely restructure the principles of intellectual property – its protection as well as its use.***
  - ***"The Future of IP", Dennemeyer, 2017***

Blockchain technology can be used to "tokenize" digital rights and could simplify the distribution of satellite generated data, analytics and imagery.

Networking and Space Community Resourcing

Coordinating space based data across sensors, networks & missions.

- Examples:
  - *NASA – Deep Space Networking and Computing – Basic Research*
  - *NASA "Sensor Web"*
  - *Network of Nodes in Space – "SpaceChain"*
  - *Open Source Networking Standard for Ground to Space Communications – "EtherSat"*



Source: NASA Website; Goddard Space Flight Center

DLT enabled communication networks could potentially improve utilization of existing space assets.

Identification Management (IdM)

Almost every industry is seeking better ways to manage identities.

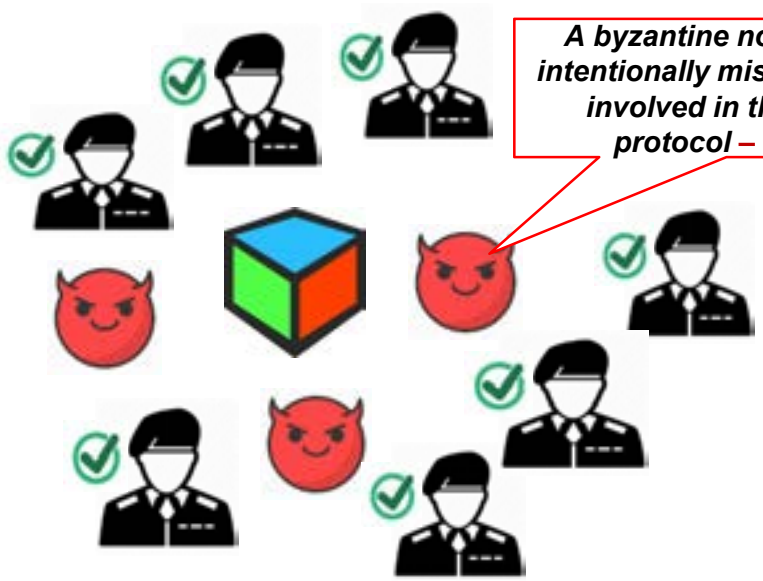
- ***The space sector depends upon secure identification for:***
  - *Authentication of employees, government officials, customers, and subscribers.*
  - *Access to networks and facilities*
  - *Access to imagery and satellite data products and communication systems*
- ***Two Types:***
  - ***Self-Sovereign Identity** – identity is controlled by the owner. (E.g. Sovrin, uPort and OneName). The Sovrin network, for instance, is an open-source decentralized identity network built on permissioned DLT. The validators or nodes could be banks, academic institutions, or another trusted institution*
  - ***Decentralized Trusted Identity** - Decentralized trusted identity provides a proprietary service that performs identity proofing of users based upon existing trusted credentials (such as a driver's license or passport) and records identity validation by DLT.*

In 2017 more than 2.9 billion records were compromised from security incidents across various industries.

With a permissionless DLT, you need to consider what happens when nodes go bad…

Byzantine Fault Tolerance – is the primary method used by blockchain network to generate chains of Hashcash style proof-of-work (or mining).

- *Mathematical proof that to tolerate n (# of malicious nodes) that you need 2n + 1 good nodes.*
- *In this case n = 3, therefore you need 7 good generals to tolerate the three bad generals*



"Byzantine General's Problem" – a situation where involved parties must agree on a single strategy in order to avoid complete failure, but where some of the involved parties are corrupt and disseminating false information or are otherwise unreliable. *(Source: L. Lamport, R. Shostak, M. Pease; SRI International; "The Byzantine Generals Problem"; 1982)*

Consensus Models: Examples

Enables mutually distrusting users to work together.

Examples	
Proof of Work - POW	• Miners solve a puzzles to “mine” a block in order to add to the blockchain. • ***Pro*** – well understood. Used by Bitcoin, Etheruem, and other cryptos. • ***Con*** - requires immense amount of energy and computational usage. • ***Reward*** - given to first miner who solves each block’s problem.
Proof of Stake - POS	• Replaces miners with validators who must lock up some of their coins as stake. Once they discover a block which they think can be added to the chain, they will validate it by placing a bet. If block gets appended, then the validators will get a reward proportionate to their bets. • ***Pro*** – energy efficient, large blockchain platforms moving to POS • ***Con*** - Only the richest stakeholders are permitted to have control of consensus • ***Reward*** - none, miners take the transaction fee
Delegated Proof of Stake - DPOS	• Anyone who holds tokens on a blockchain can select the block producers, referred to as “witnesses” through a continuous approval voting system. • ***Pro*** – scalable, energy efficient • ***Con*** – partially centralized • ***Reward*** - top 20 witnesses get paid for their services.
Round Robin	• Nodes take turns in creating blocks. Used primarily for private blockchains. • ***Pro*** – straightforward approach, no crypto puzzles, energy efficient, • ***Con*** – relies on level of trust between nodes; not appropriate for a public blockchain.

Proof of Work and Proof of Stake are the most common consensus models – but there are new models emerging. There is no perfect consensus mechanism.