Cost Analysis Needed for Blockchain Efforts

ICEAA Tampa 2019, 14-17 May 2019
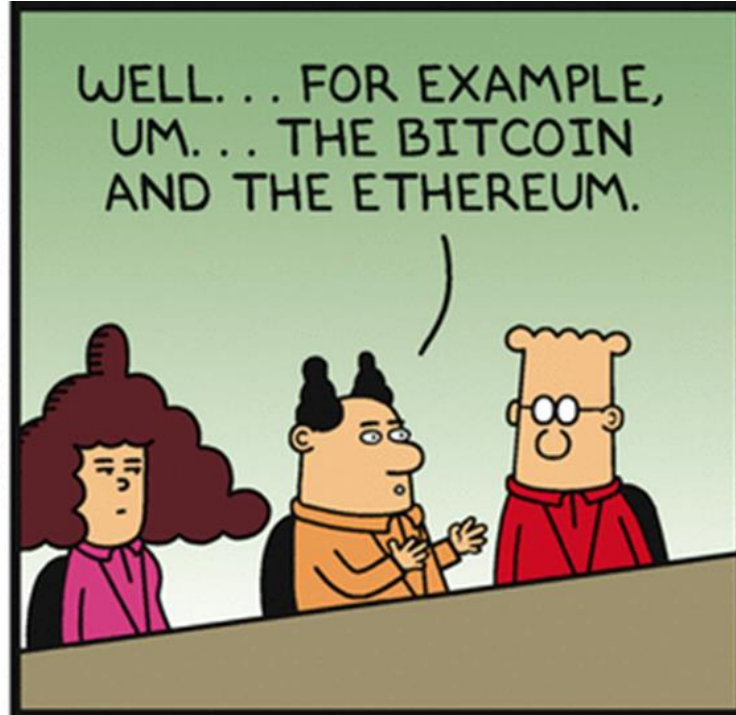
Harvey Reed

Blockchain Capability Lead

MITRE

Reference: https://dilbert.com/strip/2018-06-06

MITRE

Abstract

Cost Analysis Needed for Blockchain Efforts

Computing Track (CC05)

Harvey Reed, MITRE

U.S. government offices are exploring blockchain to address key challenges in their missions. The motivation stems from blockchain enabling peer-to-peer information sharing, without a centralized authority, which in turn supports execution of processes which span organizations. Currently, government lacks tools to describe blockchain projects with sufficient consistency to support acquisition and cost analysis. **This presentation proposes a <u>blockchain descriptive framework</u> as a first step, with a focus on cost elements and drivers for blockchain projects.**

MITRE

Outline

- **Blockchain Basics**
  - Adoption
  - Technology
  - Hypothesis
- **Blockchain Costing Descriptive Framework**
  - Cost Elements
  - Cost Drivers
  - Cost Decentralization
- **Blockchain Costing Wrap-Up**
  - Summary
  - Example Open Questions
  - Reference
  - POC

MITRE

Blockchain Basics

Adoption

Blockchain Commercial Project (circa 2018)
Global Food Safety

- **Frank Yiannis, VP Food Safety and Health, Walmart**
  - Addressed an MIT Blockchain conference in Apr 2018
  - https://thenewstack.io/walmarts-blockchain-program-may-transform-the-way-we-use-data/

- **Walmart, Nestle and many others are creating a global food safety (IBM Hyperledger blockchain) network**
  - Initial pilot used for sliced mangoes
- **Ultimate goal to provide high quality food transparency data**
  - Consortium includes: Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever and Walmart

Walmart
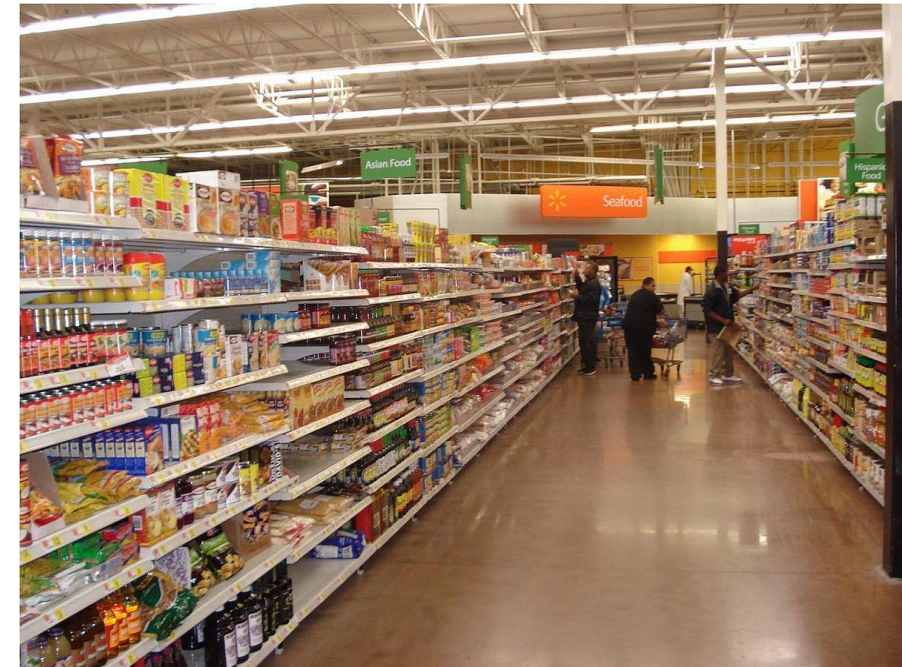
Walmart: Food Safety

https://commons.wikimedia.org/wiki/File:Walmart_grocery_section,_ethnic_foods_aisle.jpg

MITRE

Blockchain Commercial Project (circa 2018)
Oceanic Shipping

- **Maersk and other shipping companies are creating a global shipping (IBM Hyperledger permissioned blockchain) network**
  - https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/#4d5c803f05ec
  - Initial pilot tracks flower shipments
- Currently partnering with USTRANSCOM, major customer of Maersk for shipping military materiel
 - Government is a customer, learning how to use Maersk's blockchain enabled platform

**MAERSK**

However… →

Maersk: Container Shipping
https://commons.wikimedia.org/wiki/File:Maersk_Tokyo_Port_Botany.jpg

MITRE

Global Shipping Business Network (circa Nov 2018)

- **In response to Maersk being single company-centric (Maersk), CargoSmart (with Oracle blockchain) launches a blockchain-enabled consortium with the following partners:**
- **Shippers**
  - CMA CGM
  - COSCO SHIPPING Lines
  - Evergreen Marine
  - OOCL
  - Yang Ming
- **Terminal operators**
  - DP World
  - Hutchison Ports
  - PSA International Pte Ltd
  - Shanghai International Port
- **Software solutions provider**
  - CargoSmart

Credit:
https://www.cargosmart.ai/en/solutions/global-shipping-business-network/

MITRE
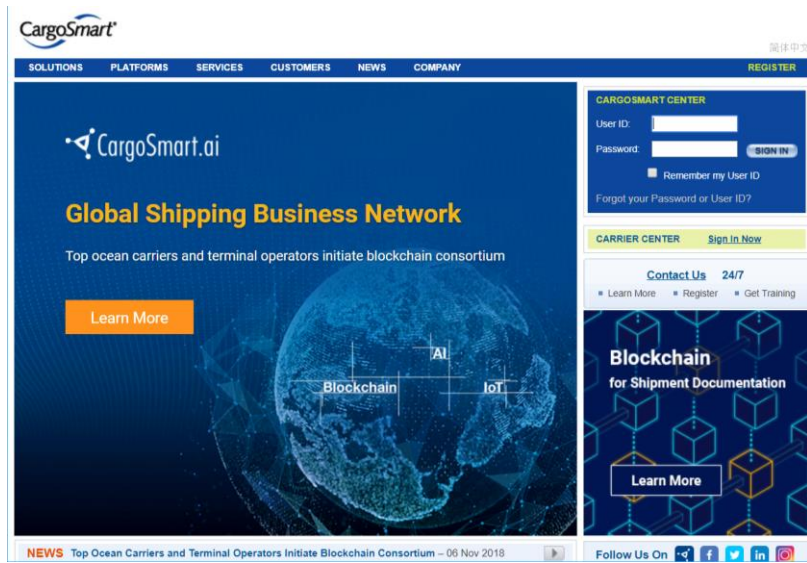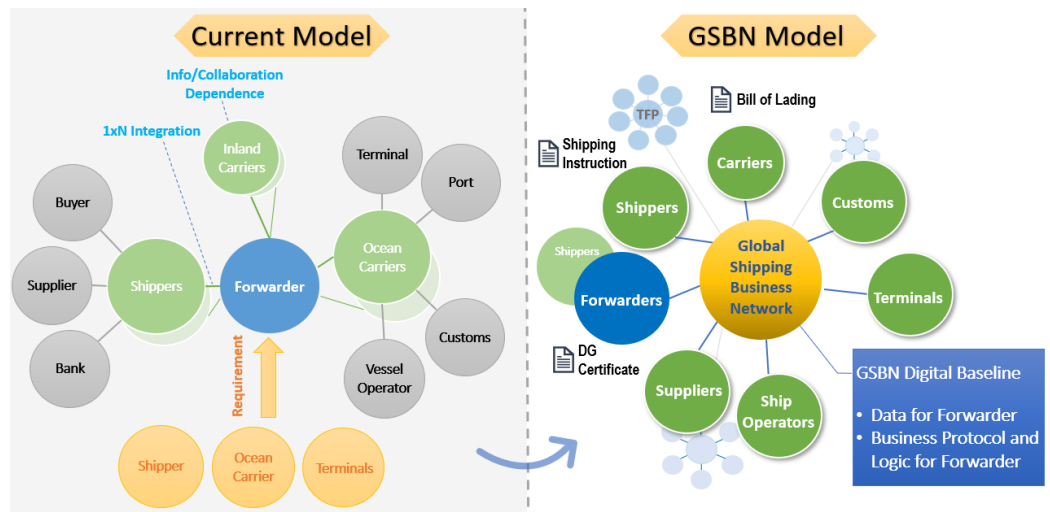
Blockchain Financial Project (circa 2018)
SWIFT Interbank Transfers

- **SWIFT completes landmark DLT PoC**
  - https://www.swift.com/news-events/news/swift-completes-landmark-dlt-proof-of-concept

- DLT (Distributed Ledger Technology a.k.a. Blockchain) Proof of Concept, using Hyperledger:
- Real time reporting
- Back office of banks need to be ready
- Standards required

The global provider of secure financial messaging services

SWIFT: Interbank transfers

https://www.swift.com/

However… →

MITRE

Ripple is Emerging as Competition to SWIFT

- **Can XRP Catch On? Ripple Touts New Banking Partnerships (Fortune 8 Jan 2019)**
  - http://fortune.com/2019/01/08/ripple-xrapid/
  - "Ripple's vision of XRP as a fast and inexpensive source of liquidity for cross-border transactions. Instead of banks having to maintain foreign bank accounts, the idea is for them to buy XRP with dollars or euros and rely on local market makers to exchange the XRP into local currencies.

    According to Graham Bright, the head of Operations at Euro Exim Bank, the process will be faster and be more transparent thanks to Ripple's blockchain technology, which creates an immutable ledger of all transactions."

Ripple

https://ripple.com/

MITRE

Government Adoption of Blockchain
HHS

- **GCN.com DEC 11, 2018**

"The Department of Health and Human Services' blockchain-powered acquisition system received its Authority to Operate on Dec. 10. HHS Accelerate, which used distributed-ledger technology, machine learning and artificial intelligence to deliver real-time information on pricing and terms and conditions from across HHS, can now go into production with live data."

HHS gets ATO for blockchain-based acquisition system

BY GCN STAFF | DEC 11, 2018

The Department of Health and Human Services' blockchain-powered acquisition system received its Authority to Operate on Dec. 10. HHS Accelerate, which used distributed-ledger technology, machine learning and artificial intelligence to deliver real-time information on pricing and terms and conditions from across HHS, can now go into production with live data.

https://gcn.com/articles/2018/12/11/arrieta-hhs-accelerate.aspx

MITRE

Blockchain Basics

Technology

MITRE

Technology Foundation

- **Blockchain records transactions**
  - In cryptographically secure blocks of transactions…
  - Stored on decentralized servers

- **Blockchain available in**
  - Public and
  - Permissioned variants

- **Govt will likely start with permissioned blockchains**
  - Similar to commercial permissioned blockchain efforts

MITRE

Tamper Resistant Blockchain

Figure 1. Blocks are linked by the hash of their contents

Figure 1 from Blockchain for government (Bryson, et al, Apr 2018):
https://www.mitre.org/publications/technical-papers/blockchain-technology-for-government

MITRE

Public and Permissioned Blockchains

Likely more suitable for government use ➡️

Permissioned Blockchain
e.g. Tendermint, Hyperledger Fabric

BFT consensus (Byzantine Fault Tolerance)

Public Blockchain
e.g. Bitcoin, Ethereum

Nakamoto consensus (Proof of Work)

Table 1. Consensus comparison

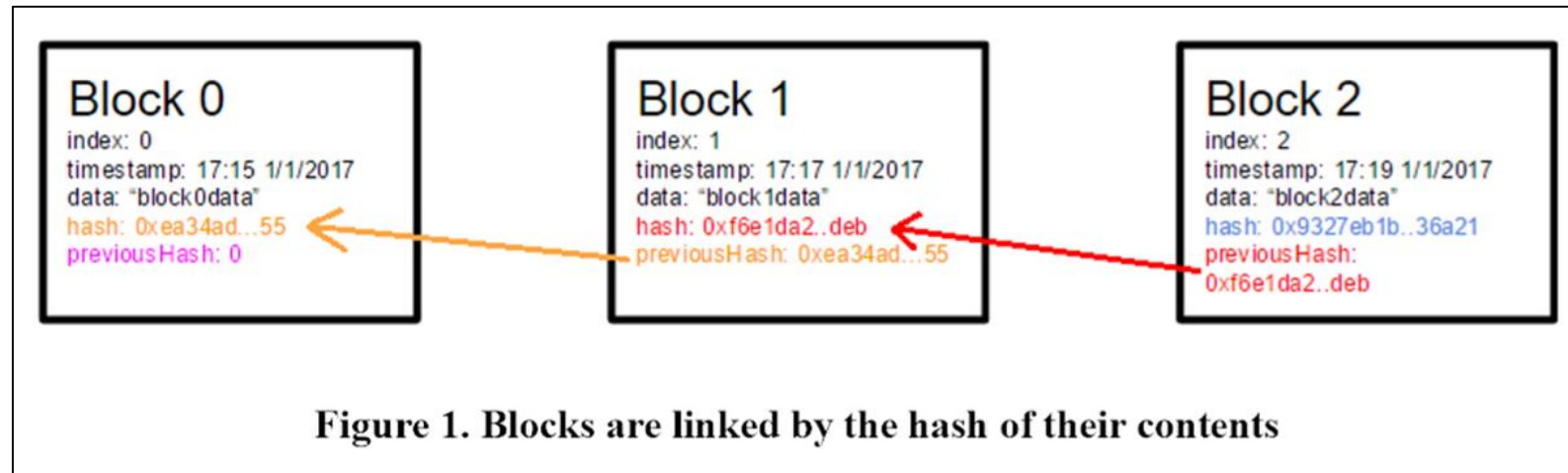|	BFT	Nakamoto
Speed (transactions per second)	**Potentially 1000s**	< 20 on average
Network Scalability	**100s of nodes**	**1000s of nodes**
Block Finality	**Instant**	**Eventual**

Table 1 from Blockchain for government (Bryson, et al, Apr 2018):
https://www.mitre.org/publications/technical-papers/blockchain-technology-for-government
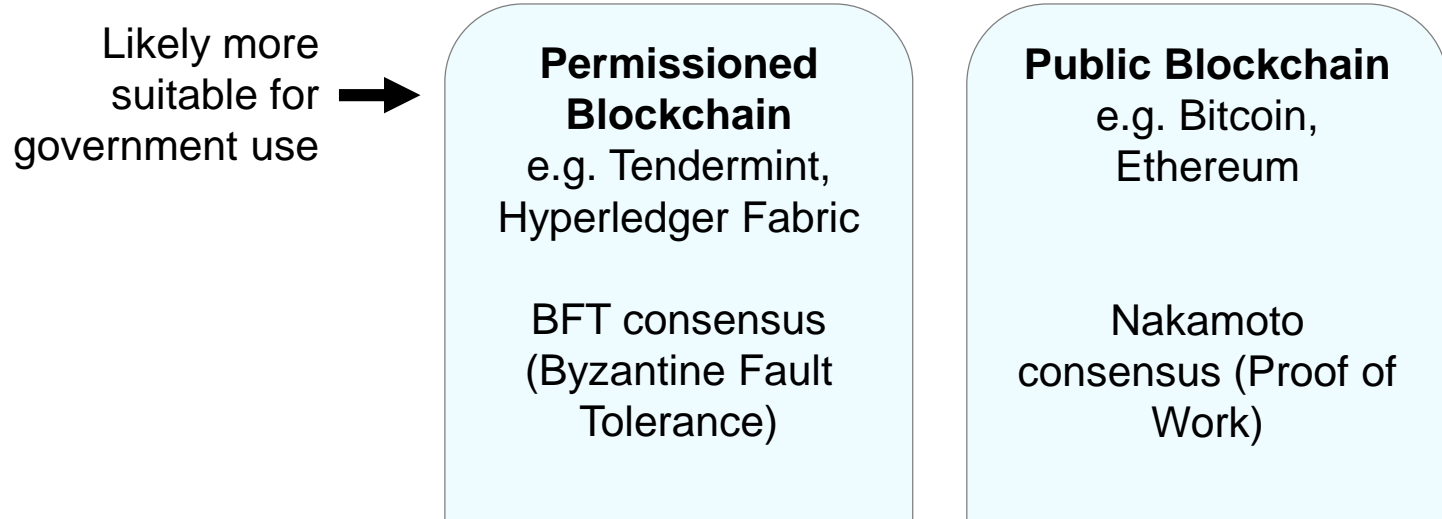
MITRE

Notional Govt Permissioned Blockchain

- **Mission oriented permissioned blockchain is a shared capability**
- **Blockchain serves as an alternative to expensive and ineffective "many-to-many" identity and access federation strategies**
  - Cost of adding partners increases over time if each new partner needs to add all other partners to participate
  - With blockchain, each partner adds just one entity, the blockchain

MITRE
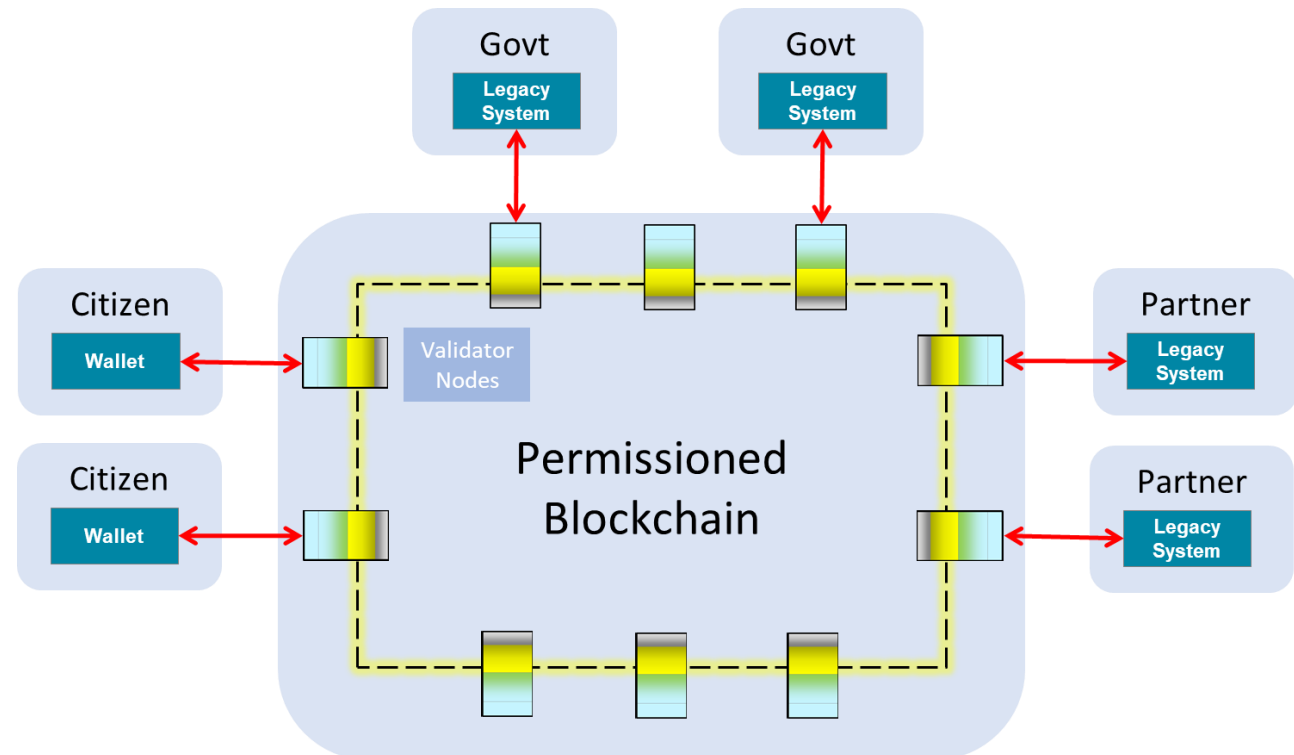
Blockchain Basics

Hypothesis

MITRE

Govt Permissioned Blockchain

Mission stakeholders improve mission effectiveness by sharing validated transactional information across untrusted boundaries between stakeholders
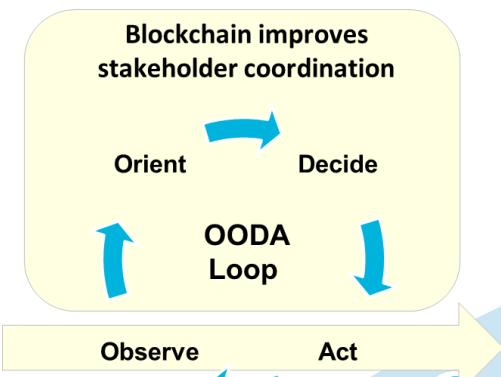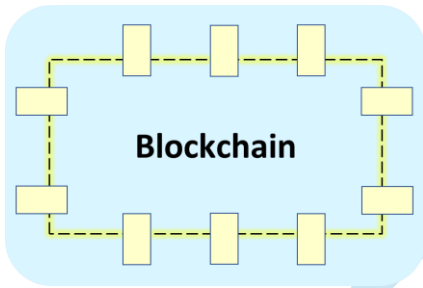
Blockchain improves stakeholder coordination

Orient → Decide

OODA Loop

Observe — Act

Mission Effectiveness

Improve mission effectiveness

Improve situational awareness

Blockchain

Capture transactional data in real time
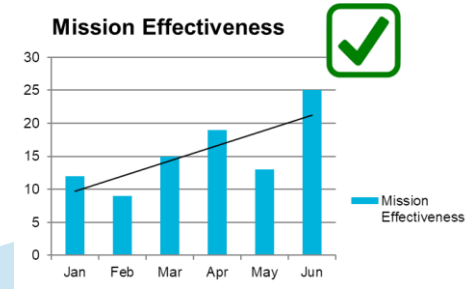
All blockchains must support an improvement to mission effectiveness

MITRE

Mission Improvement – Connect With Value Statement

- **Value of Sharing information**
  - Decentralized, autonomous collection of data into a permissioned blockchain vs. centralized hierarchical means of collection into disparate legacy systems
  - Improves decision cycle
- **Value of Coordination**
  - Trusted transactional data gives transparency to processes shared among stakeholders vs. legacy federation and info sharing among orgs
  - Enables new stakeholder processes on top of the permissioned blockchain

Mission Effectiveness

Blockchain improves stakeholder coordination

Orient — Decide
OODA Loop
Observe — Act

Improve mission effectiveness

Improve situational awareness

Blockchain

Capture transactional data in real time
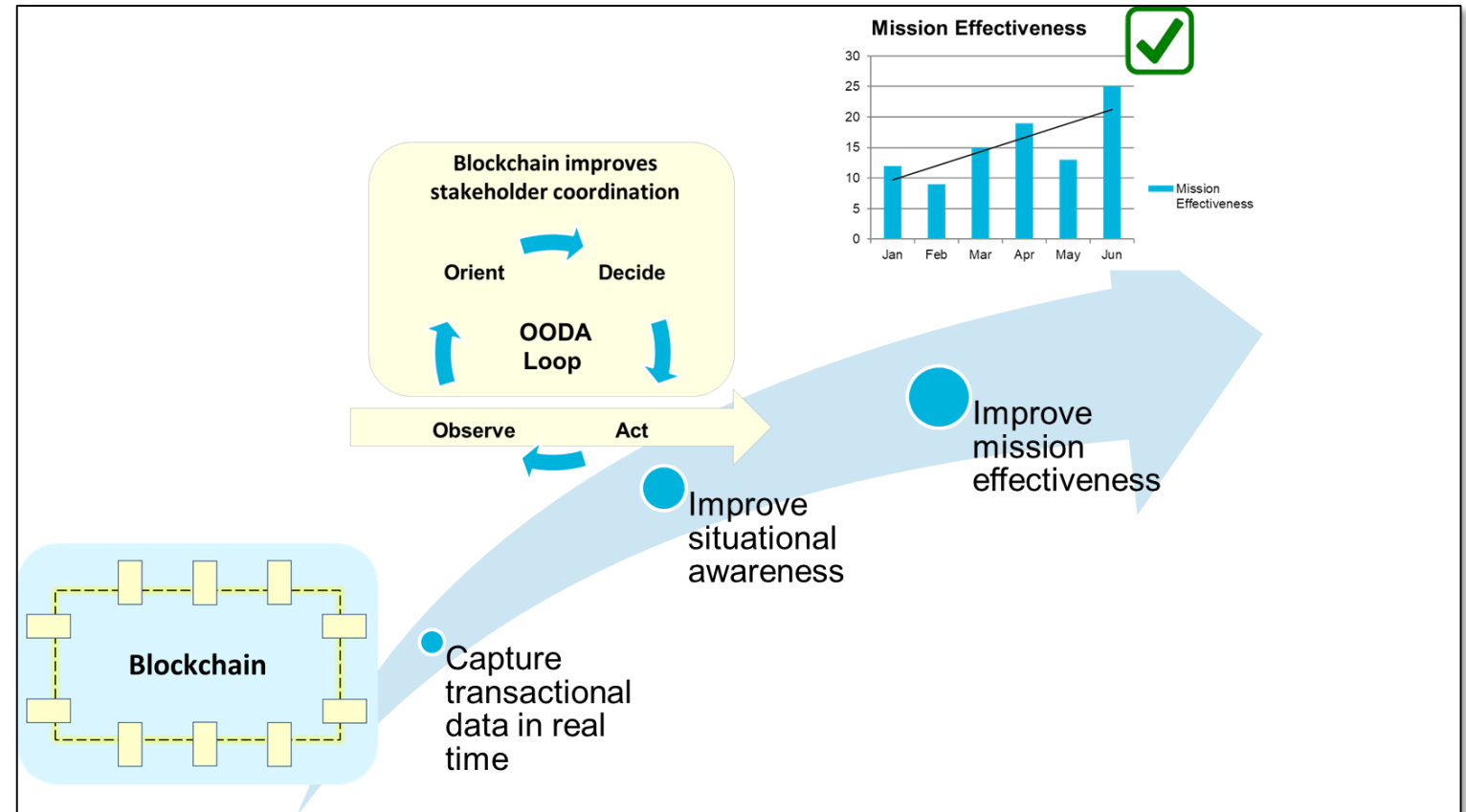
Govt Permissioned Blockchain Hypothesis

MITRE

Realize Value – Standup a Permissioned Blockchain

- **A permissioned blockchain effort requires standing up a blockchain**
  - Vice using an existing public blockchain

- **Standing up a permissioned blockchain should start with open source**
  - (else face a huge steep learning curve)
  - And should focus on add-ons and configuration

- **Permissioned blockchains require hosting environment(s)**
  - Where diverse locations and environments can mitigate a variety of threats

MITRE

Key Components of Blockchain Technology

- **From:**
  - https://www.mitre.org/publications/technical-papers/blockchain-technology-for-government
- **Blockchain can be assembled from open source projects, commercial, or both**
- **Later slides will cover relevant integration and enterprise aspects**

MITRE
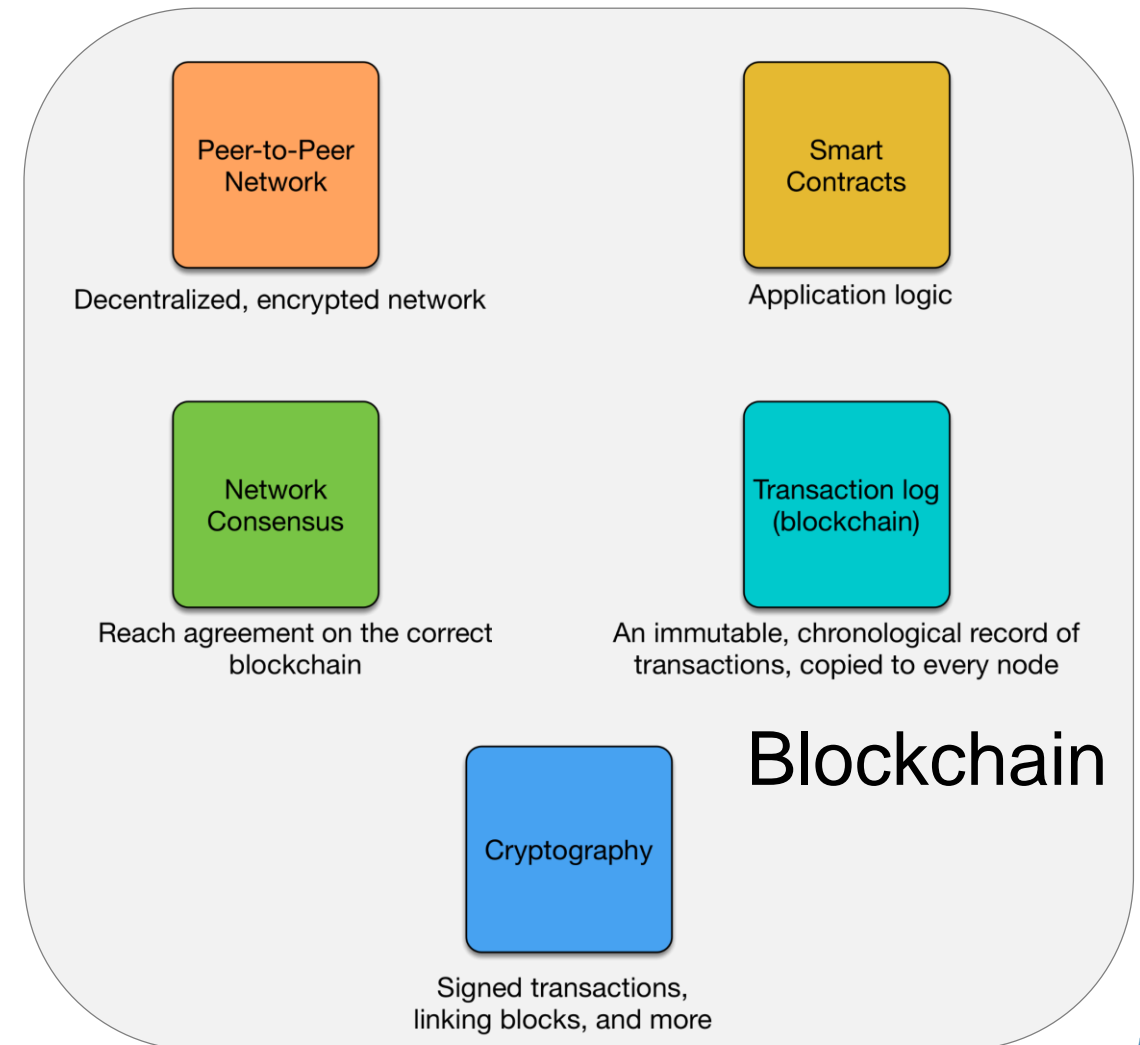
# Operate a Permissioned Blockchain

- **A permissioned blockchain is operated by key stakeholders**
  - (vice centralized owner/operator legacy model)
  - And requires governance

- **A permissioned blockchain is sustained by hosting stakeholders**
  - To implement maintenance, e.g. IAVAs (Information Assurance Vulnerability Alert)
  - As well as rollout improvements (e.g. new smart contracts)

MITRE

Operation, Sustainment, Governance

- **Govt and partner organizations own and operate nodes as needed, per agreement**
- **Same organizations responsible for cyber maintenance (e.g. IAVAs [Information Assurance Vulnerability Alert] a.k.a. "security patches")**
- **One or more organizations responsible for software dev and updates, rolled out to other operator org nodes**
- **Citizens and other end users are (in general) not responsible for operation or sustainment**
- **Governance required to codify roles and responsibilities among stakeholders**

MITRE
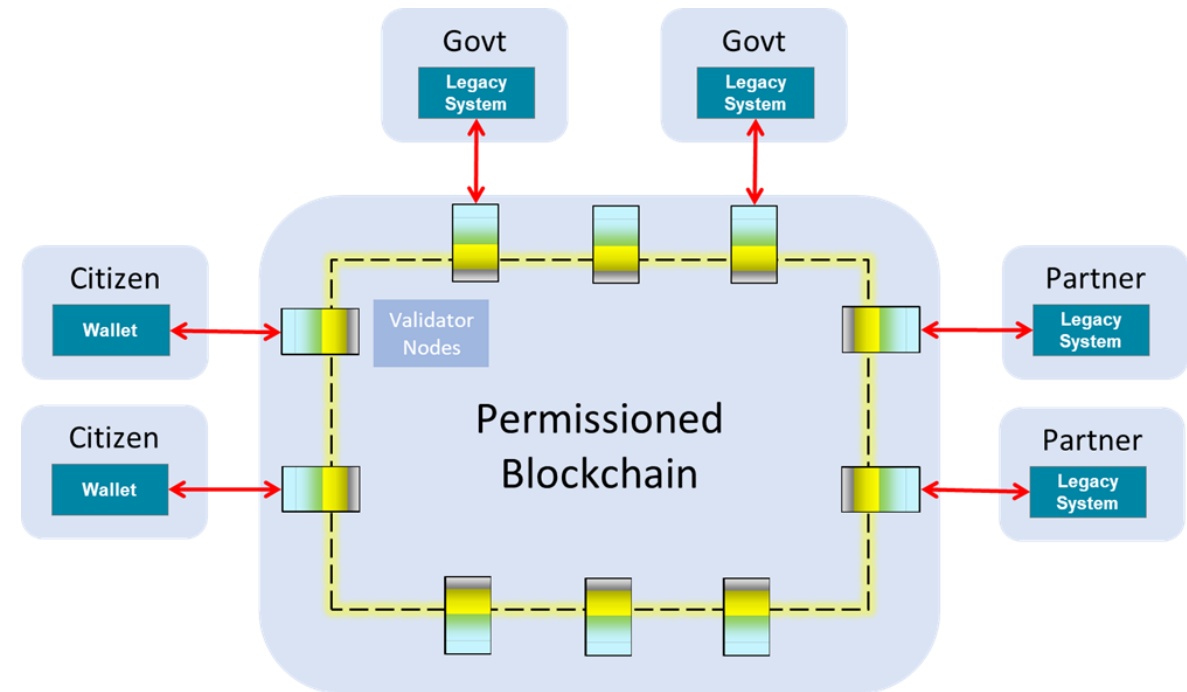
Putting It All Together

- **Blockchain enables a community of stakeholders to directly connect to the blockchain**

  – Transactional data is consistently validated

  – Data is tamper-evident

  – Data is protected against destruction

Legacy
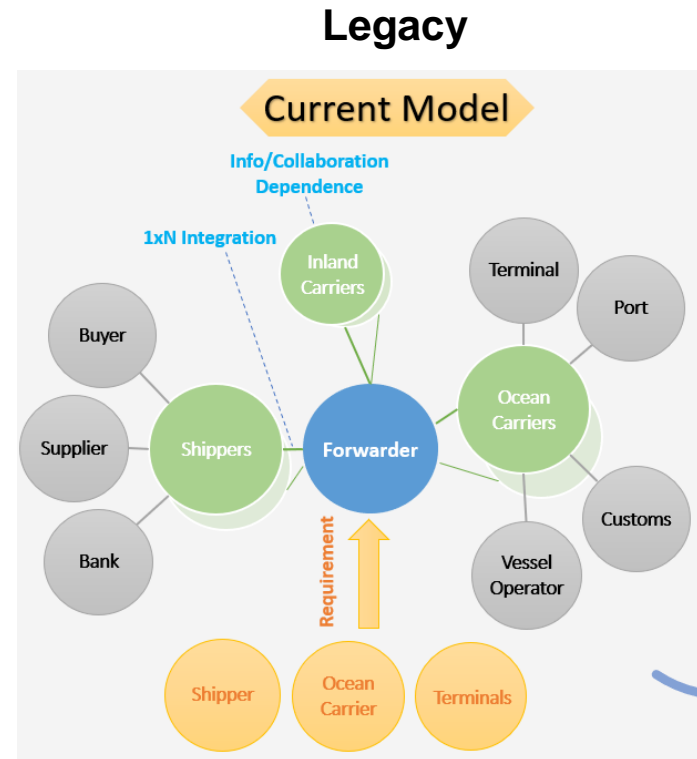
- Complex machine to machine data sharing relationships
- Connections are 1 : many – partner to partner to partner…

Blockchain-Enabled
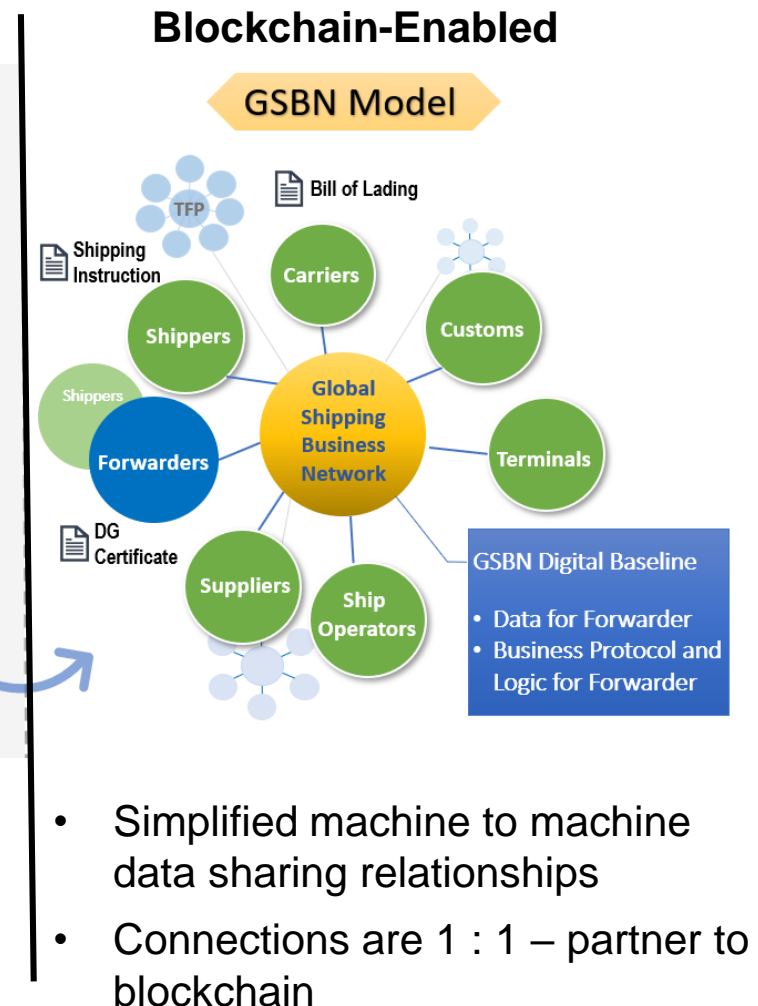
- Simplified machine to machine data sharing relationships
- Connections are 1 : 1 – partner to blockchain

Example from CargoSmart (slide 8)

MITRE

Blockchain Costing Descriptive Framework

Cost Elements

Top level survey of cost elements in a blockchain which incur costs

MITRE

Cost Elements (1 of 3)
High Level

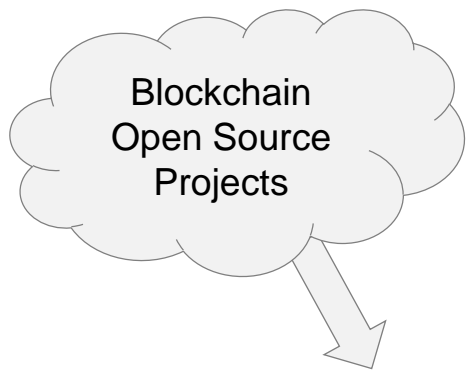| Component	Cost Element
Select blockchain open source project	**Large item:** Requires thorough analysis of the core needs, consensus, anticipated threats, performance, etc. Should be described in the context of a mission oriented hypothesis. Must choose which metrics and mission outcomes define success.
Incorporate blockchain into capability	**Very large item:** The full capability incorporates interfaces, new processes (see OODA Loop above), reporting, analytics, etc. Recommend iterative delivery of capability. Most likely will never have full requirements at the start.
Negotiate with stakeholders	**Medium item:** Stakeholder agreement required for functionality, operation, and sustainment. Starts early. All stakeholders involved in decision making through dev / test / rollout / operations, etc.

Also see stakeholder cost driver

Select open source blockchain project:
Open source is "free" but like any open source project need to account for additional GOTS (government-off-the-shelf) software, integration, etc.

Blockchain Open Source Projects

Incorporate blockchain in capability:
Wrapping blockchain with interfaces, new processes, reporting, etc.

Negotiate with stakeholders:
Stakeholder agreement required for functionality, operation, and sustainment

Govt Legacy System

Govt Legacy System

Citizen Wallet

Validator Nodes

Permissioned Blockchain

Partner Legacy System

Citizen Wallet

Partner Legacy System

MITRE
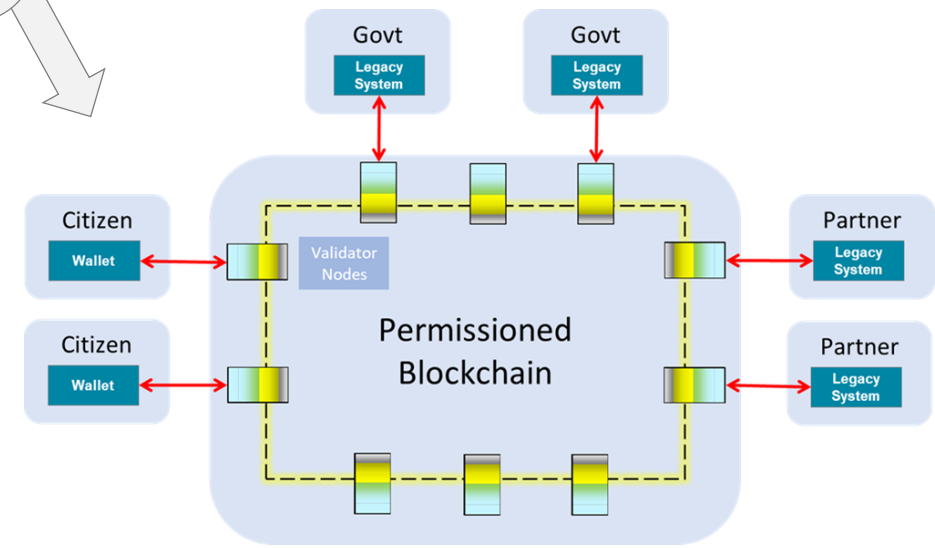
Cost Elements (2 of 3)
Detail

Component	Cost Element
Peer-to-peer network	n/a Usually part of blockchain open source
Network consensus	n/a Usually part of blockchain open source
Cryptography	n/a Usually part of blockchain open source

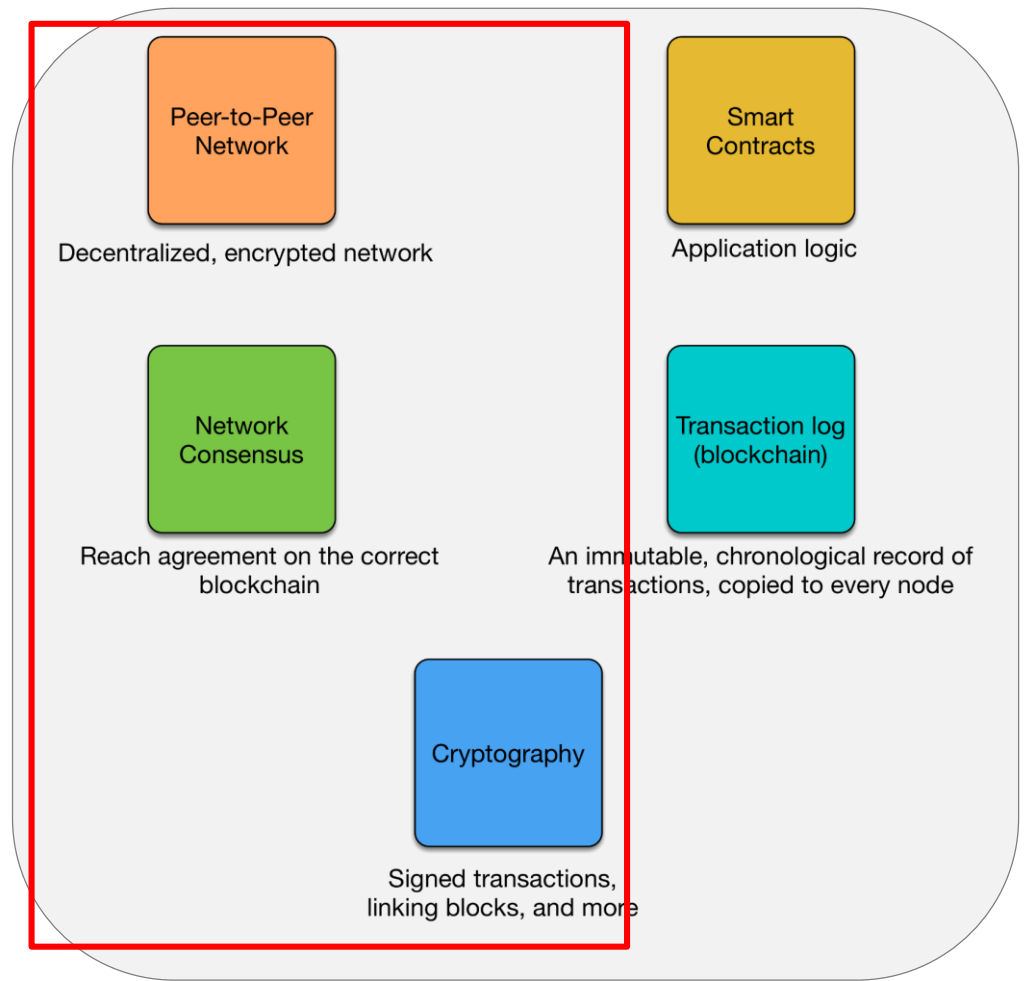**Selecting open source blockchain (above) determines certain blockchain components:**
While technically possible to "swap out" modules such as consensus, this is not recommended. Same with P2P communications and cryptography. Blockchains inherently integrate the components.

Blockchain

Peer-to-Peer Network — Decentralized, encrypted network

Smart Contracts — Application logic

Network Consensus — Reach agreement on the correct blockchain

Transaction log (blockchain) — An immutable, chronological record of transactions, copied to every node

Cryptography — Signed transactions, linking blocks, and more

MITRE

Cost Elements (3 of 3)
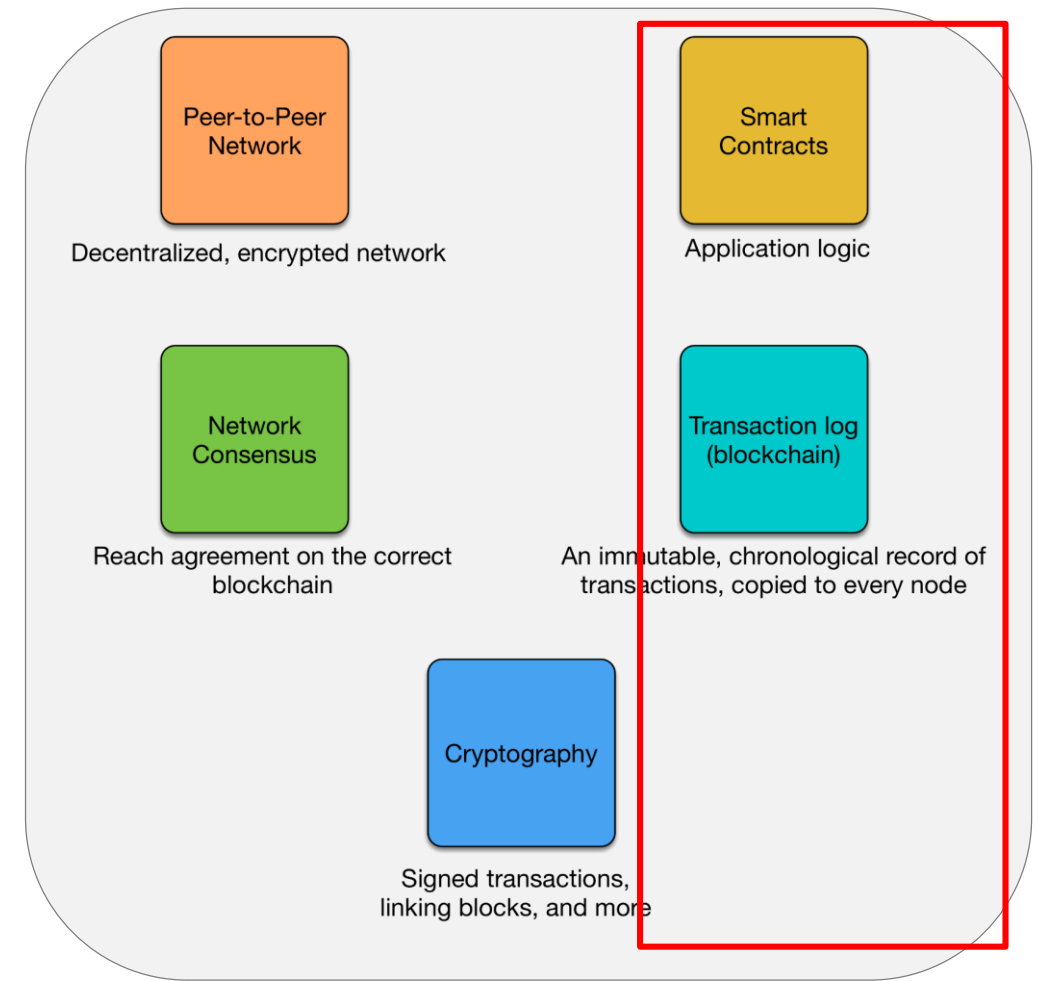## Detail

Component	Cost Element
Application logic	**Large item:** Smart contracts execute in blockchain and requires extensive design and testing. Blockchain transactions are final. Additional application logic (executes outside of blockchain) works with smart contracts, and constitutes new processes (see OODA Loop above) which is the bulk of value of the blockchain.
Transaction log	**Large Item:** Transaction data needs design, and correlation with anticipated (legacy) data sources. Once designed, blockchain transactions require standing up, owning and operating blockchain servers to capture blockchain transactions as written.

Also see process cost driver

Also see data cost driver

Selecting open source blockchain (above) leaves logic and transaction design open:
Blockchain will provide a framework for logic and transaction design, which dev / test will use to achieve mission performance.

Blockchain

Peer-to-Peer Network
Decentralized, encrypted network

Network Consensus
Reach agreement on the correct blockchain

Smart Contracts
Application logic

Transaction log (blockchain)
An immutable, chronological record of transactions, copied to every node

Cryptography
Signed transactions, linking blocks, and more

MITRE

Blockchain Costing Descriptive Framework

Cost Drivers

Cost drivers indicate trends of increased or decreased costs dependent on scale of use

MITRE

Scaling Cost Drivers – Stakeholder Diversity

- **Stakeholder diversity**
  - All U.S. govt?
  - State, local, tribal govt?
  - Citizens?
  - Other countries?
  - One governance or layered?
- **Impact**
  - Increased stakeholder diversity gives greater assurance that stakeholders are included
  - Increased diversity requires upfront investment to assure all needs are being met
 - Increased cost

MITRE
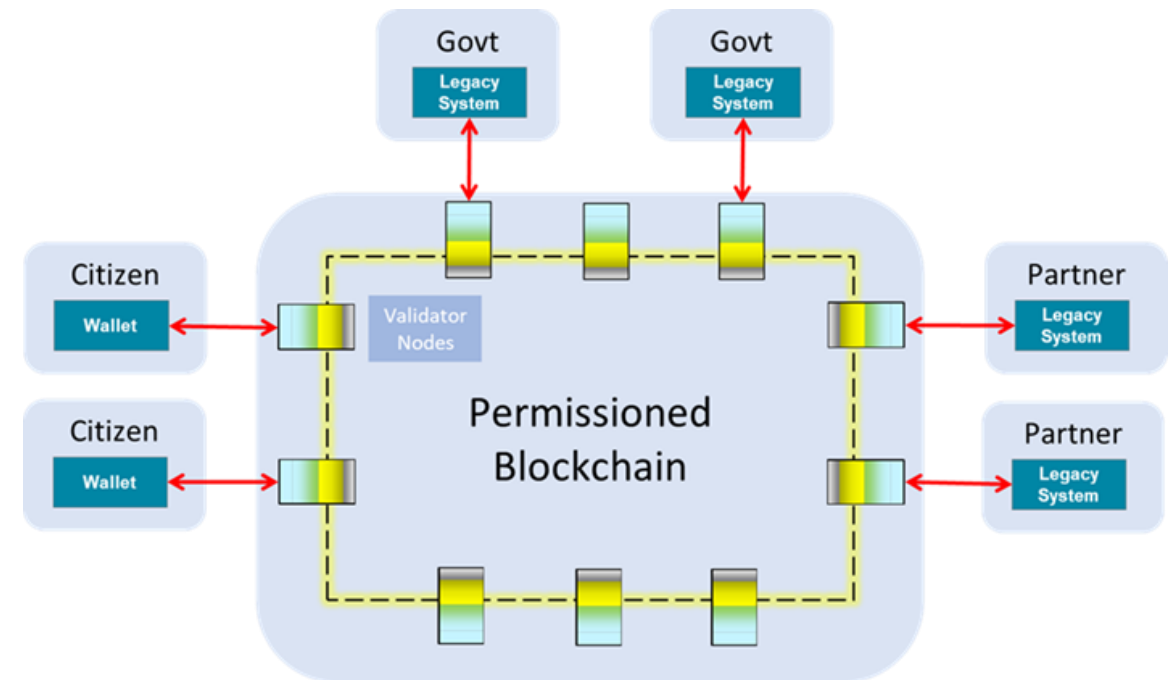
Scaling Cost Drivers – Data Diversity

- **Data diversity**
  - Number of data sources for blockchain transactions
  - Blockchain transactions (at least initially) come from legacy sources which have different methods of packaging and interpreting data (syntax, semantics)
  - Data crosses security regimes
- **Impact**
  - Increased data diversity gives greater assurance that all data needed for new processes are included
  - Increased data diversity requires upfront investment to assure all data is understood
  - Increased cost

MITRE
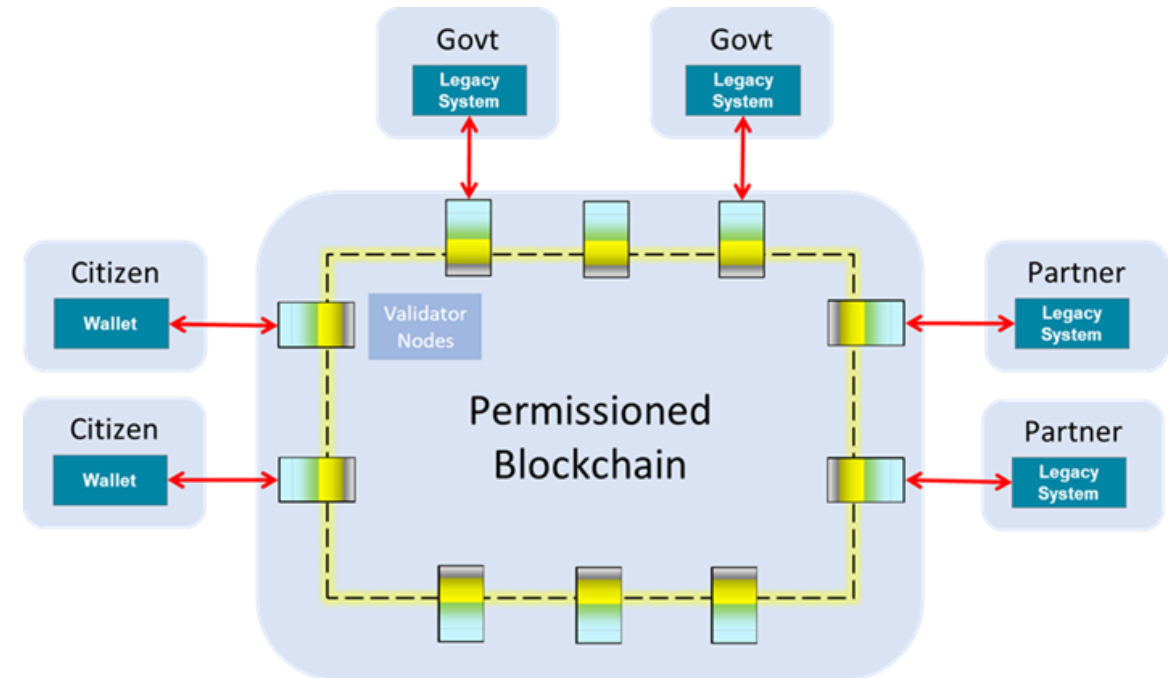
Scaling Cost Drivers – New Processes

- **New processes (and smart contracts)**
  - New processes are the source of value of the blockchain and enable stakeholder coordination
  - Mission outcomes and effectiveness are dependent on new processes (see OODA Loop above)
  - Incremental rollout (see below) of blockchain enabled capability is dependent on incremental rollout of new processes (limiting factor)
- **Impact**
  - New processes deliver mission value
  - New processes were never before feasible (by definition, else would not need blockchain) thus will be new to test (not duplicating legacy function), requiring new investment
  - Increased cost

MITRE
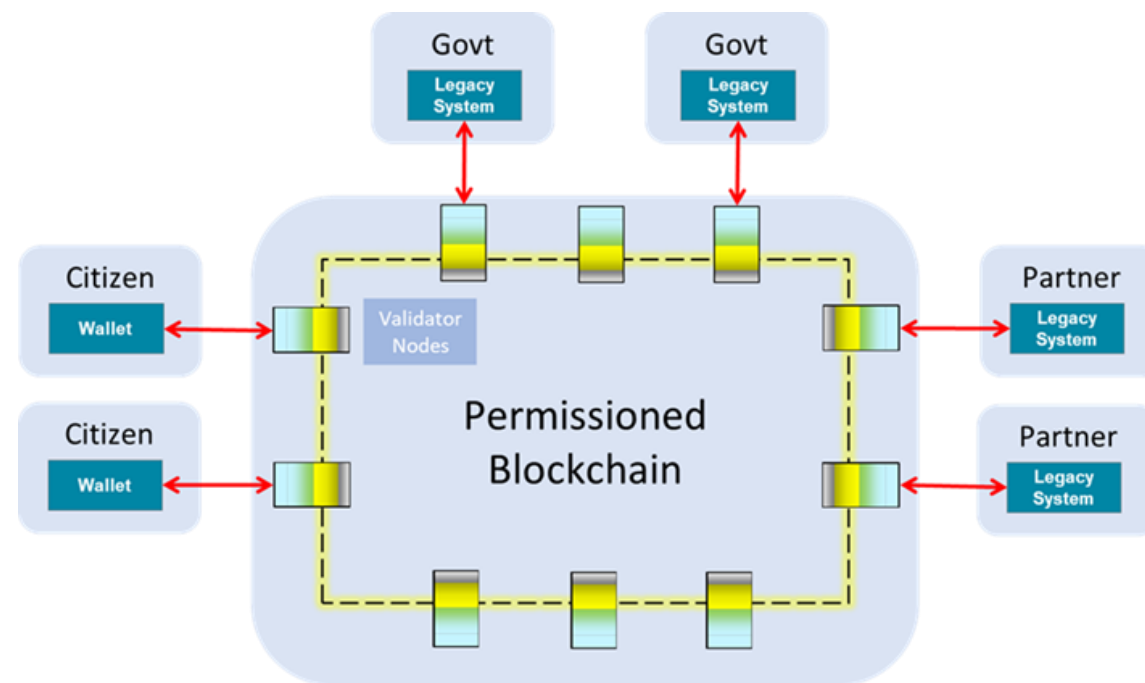
Scaling Cost Drivers – Continual Innovation

- **Incremental roadmap (vice block delivery)**
  - Incremental delivery lowers risk for rework
  - Includes incremental:
    - Addition of stakeholders
    - Addition of legacy systems
    - Addition of new processes (and smart contracts)
  - Roadmap of annual execution plans (vice block delivery)
- **Impact**
  - Reduce rework
  - Maintain forward momentum
  - Build confidence with each delivery
  - Adjust culture of all stakeholders incrementally
 - Reduced overall cost (compared to large block delivery)

Grow the Blockchain

Deliver "Minimum Viable Product" (agile) Add-ons

Add   **Add**   **Add**   **Add**

MITRE

Blockchain Costing Descriptive Framework

Cost Decentralization

MITRE

Blockchain Cost is Decentralized

- **Classic standalone systems have highly centralized costs, e.g. for C2 systems:**
  - The PEO (acquisition)
  - The user(s) (owner/operator)
- **Blockchain is decentralized**
  - Acquisition (may be governed by stakeholders)
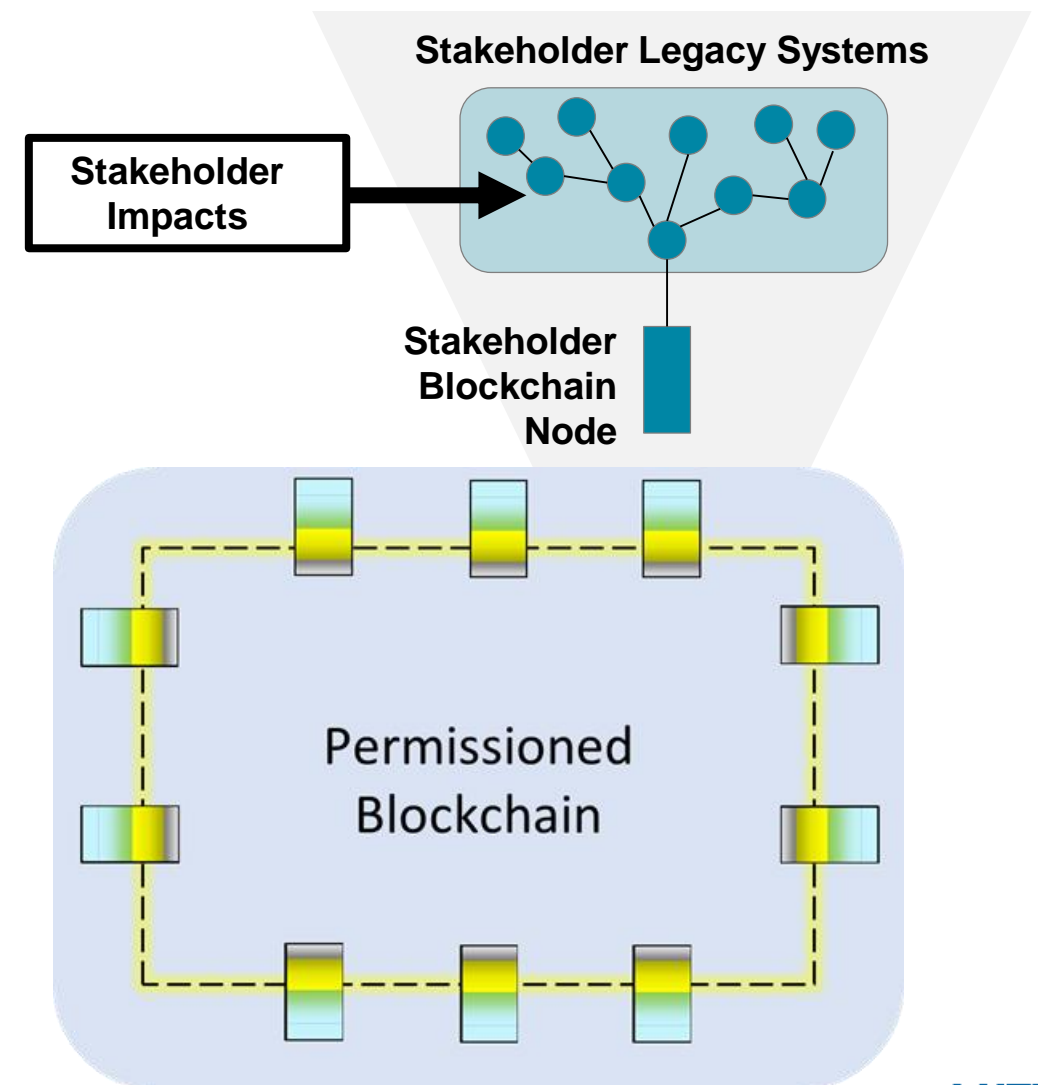 - Owner/operator (potentially every stakeholder organization)
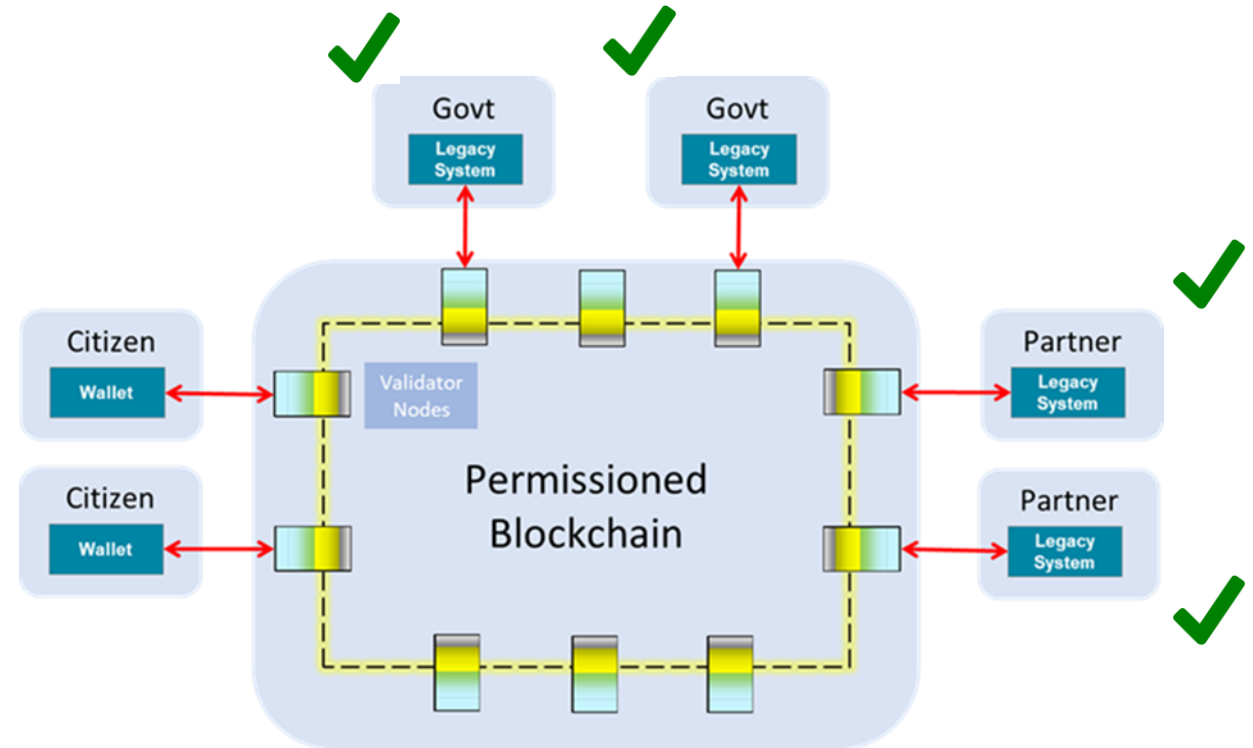
Stakeholder Cost

- **Stakeholder costs**
  - Every stakeholder needs to adjust their backend systems
 - Costs will vary
- **Rationale**
  - Most / all stakeholders have a means to represent the implicit community processes in their own (siloed) systems
  - With blockchain, stakeholders can now use the blockchain and new processes to know the status of community processes
  - This shift in process representation responsibility may (likely) require rework in each stakeholders' backend legacy systems
  - Costs will vary

Stakeholder Legacy Systems

Stakeholder Impacts

Stakeholder Blockchain Node

Permissioned Blockchain

MITRE

Blockchain Costing Wrap-Up

MITRE

Summary

- **Cost Elements**
  - High-level blockchain cost
  - Blockchain components
- **Cost Drivers**
  - Stakeholder diversity
  - Data diversity
  - New processes
  - Incremental roadmap
- **Cost for Stakeholders**
  - Stakeholder legacy system impact
- **Open Cost Questions**
  - Next slide

Blockchain Components

Blockchain Node

Blockchain software, AI, hardware

MITRE
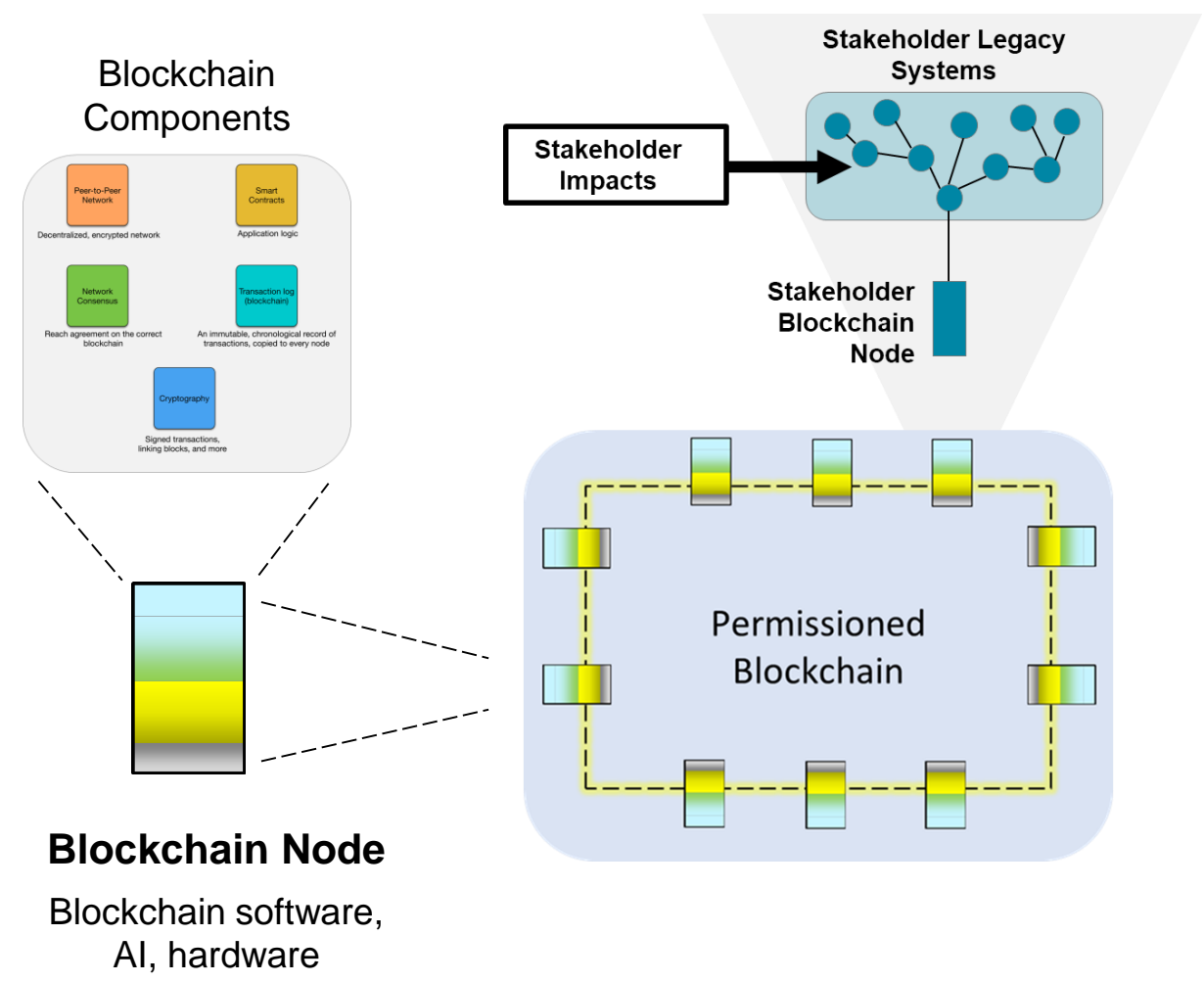
Example Open Questions

- **Technology**
  - New blockchain variants with improved performance
  - New decentralized files systems, complementary to blockchain
- **Policy**
  - Govt policy (or regulation) pro/con blockchain?
- **Shared Service**
  - GSA shared blockchain?

MITRE

References

- **"The Emergence of Trust and Value in Public Blockchain Networks," Michael Norman, Yiannis Karavas, Harvey Reed, June 4 2018, poster session for The Ninth International Conference on Complex Systems (ICCS 2018), public release case number 18-1814**

- **"Blockchain Technology in Government," Dave Bryson, David Penny, David Goldenberg, Gloria Serrao, Dec 2017, public release case number 18-1069. (https://www.mitre.org/publications/technical-papers/blockchain-technology-for-government)**

MITRE

POC

Harvey Reed

Blockchain Capability Lead

The MITRE Corporation

hreed@mitre.org

781-439-7666 (mobile)

Computing Track: Cost Analysis Needed for Blockchain Efforts (CC05)

Harvey Reed is the MITRE Blockchain Capability Lead and champions the use of open source blockchain technology, software reuse and assembly, and rapid develop and deploy methodologies. Currently focused on development of opportunities, addressing challenges, and mitigation of risks for government adoption of blockchain across multiple domains.

MITRE

MITRE

MITRE is a not-for-profit organization whose sole focus is to operate federally funded research and development centers, or FFRDCs. Independent and objective, we take on some of our nation's—and the world's—most critical challenges and provide innovative, practical solutions.

Learn and share more about MITRE, FFRDCs, and our unique value at www.mitre.org

MITRE