Costing Blockchains

Wed 7 Nov 18 at 11:30 – 1:00 PM ET

Harvey Reed
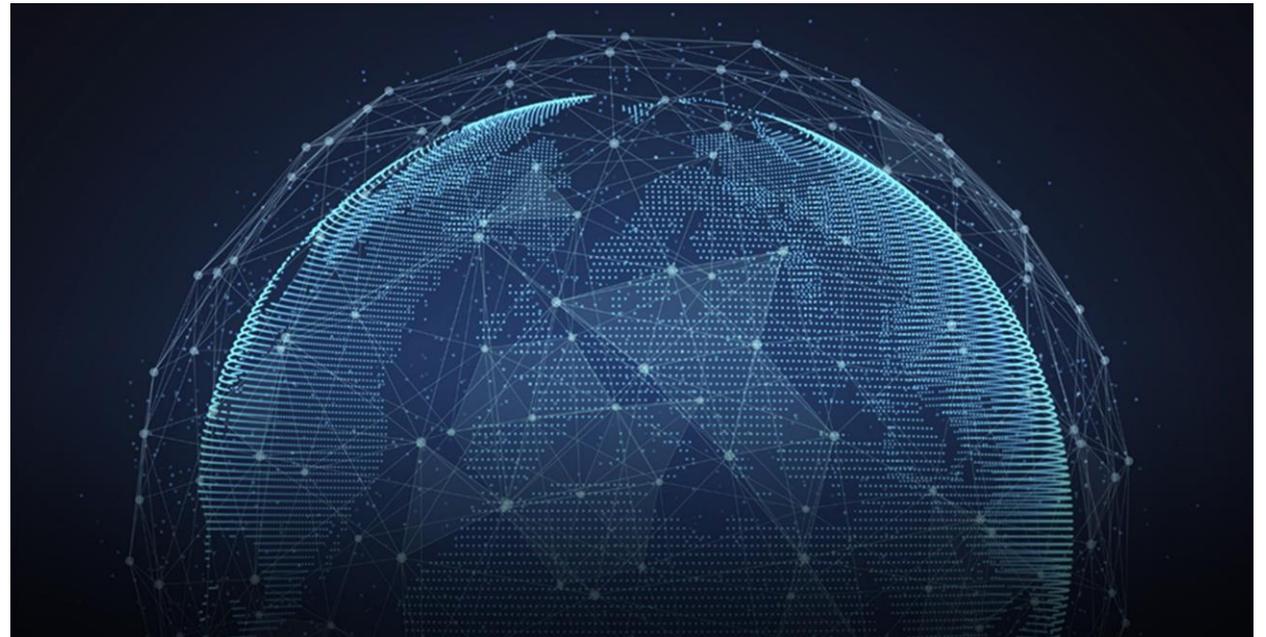
Blockchain Capability Lead

MITRE

Skype:

https://meet.mitre.org/kcincotta/W3J0216Y

ID: 689801244

MITRE

Welcome

- **ICEAA (International Cost Estimating and Analysis Association)**
  - Timothy P. Anderson, CCEA, Director, Integrated Cost and Schedule Analysis (iCASA), The Aerospace Corporation

- **MITRE**
  - Kevin Cincotta, co-lead of Cost Analysis CoP, MITRE
  - Harvey Reed, Blockchain Capability Lead, MITRE (speaker)

MITRE

Abstract

- **This brief reviews blockchain basics (e.g. technology foundation, standup a permissioned blockchain, operate blockchain), followed by a survey of cost elements, cost drivers, and cost questions.**

- **It is intended as an introduction for an acquisition and cost audience.**

- **Blockchain technology is still emerging, and the state of blockchain standards and practices is nascent and rapidly evolving.**

MITRE

References Available Upon Request

- **"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/sites/default/files/publications/blockchain-technology-for-government-18-1069.pdf)**

MITRE

Blockchain Basics

Caution: blockchain technology is rapidly evolving

MITRE

Commercial Adoption of Blockchain

- **From hype:**
  "best thing since sliced bread"

- **To reality:**
  several impactful permissioned blockchain pilots in progress – food safety, shipping, international bank transfers, and more

- **Examples described in backup slides**

Wal-Mart: Food Safety

The global provider
of secure financial
messaging services

SWIFT: Inter-bank transfers

Maersk: Container Shipping

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

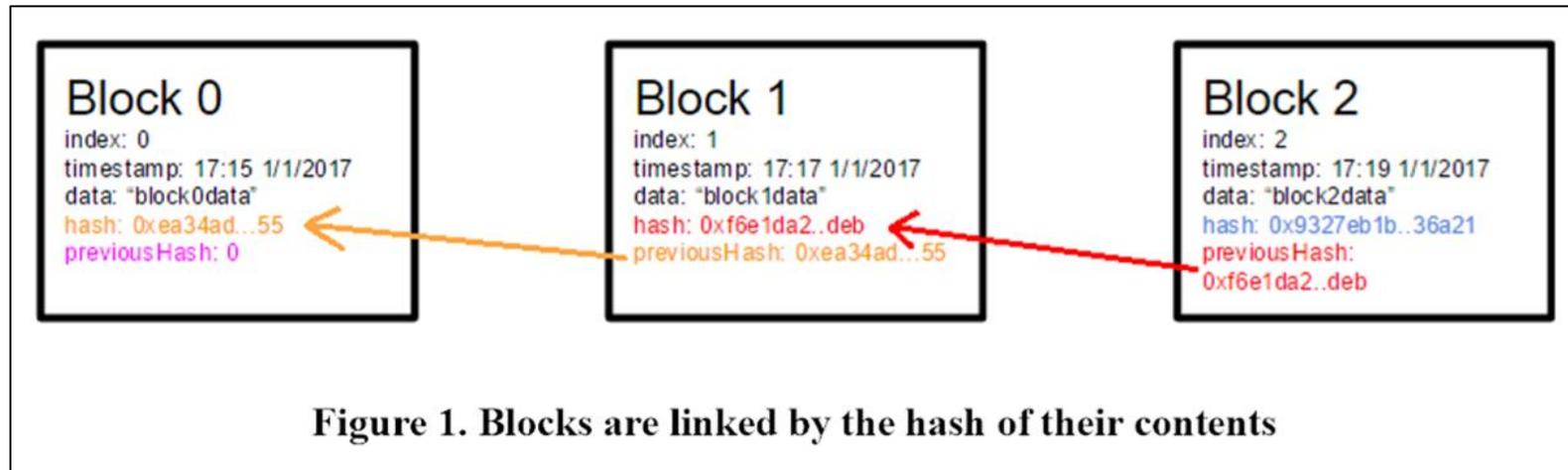
Figure 1. Blocks are linked by the hash of their contents

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

Public Blockchain

e.g. Bitcoin, Ethereum

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" federation strategies**

MITRE
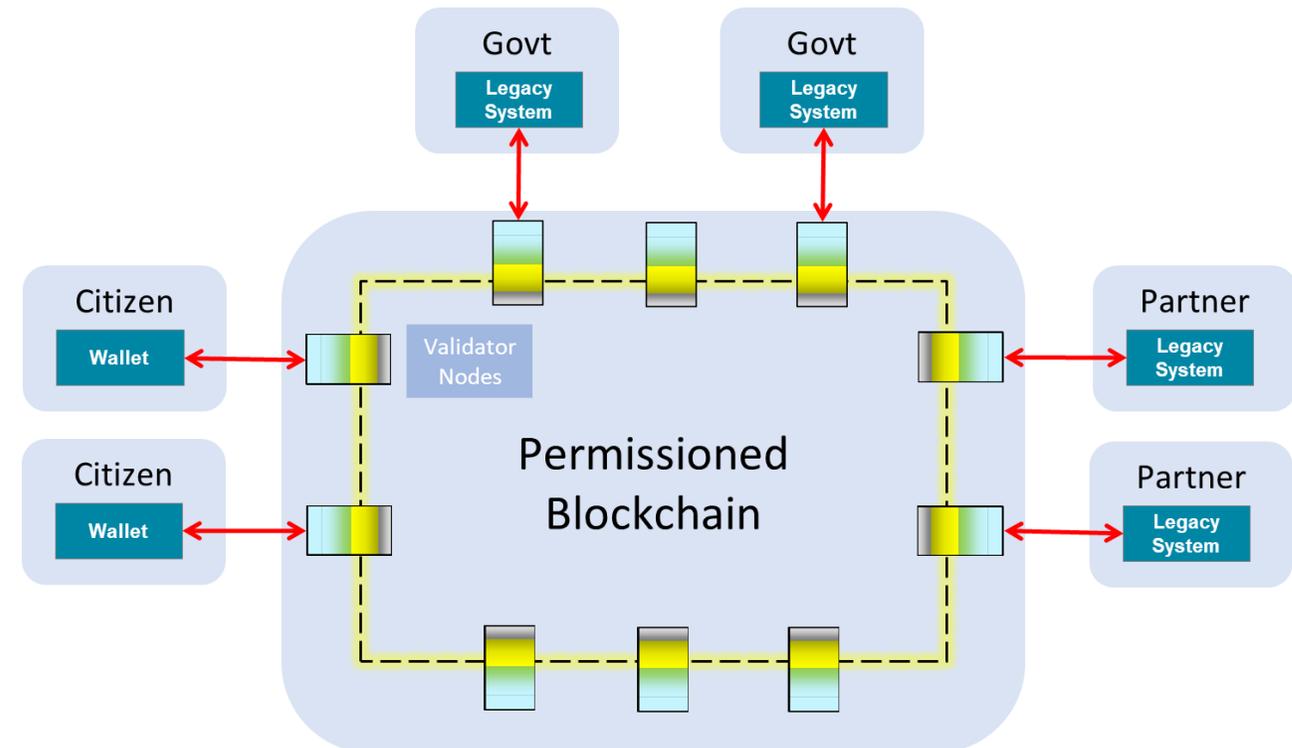
Govt Permissioned Blockchain

Mission stakeholders improve mission effectiveness by sharing validated transactional information across untrusted boundaries between stakeholders

Mission Effectiveness

Blockchain improves stakeholder coordination

Orient → Decide

OODA Loop

Observe — Act
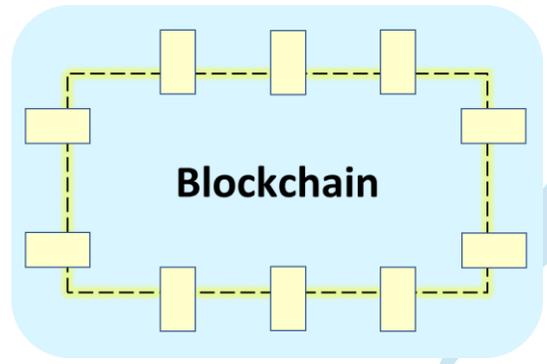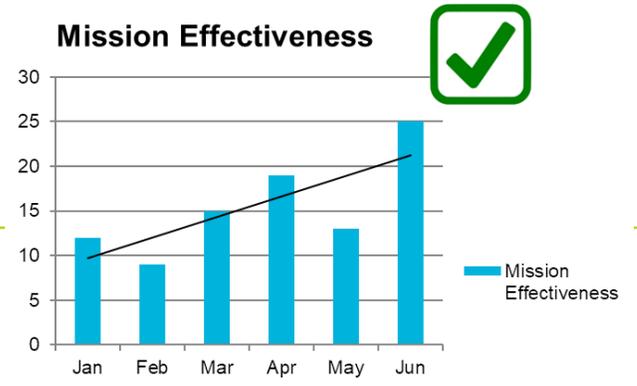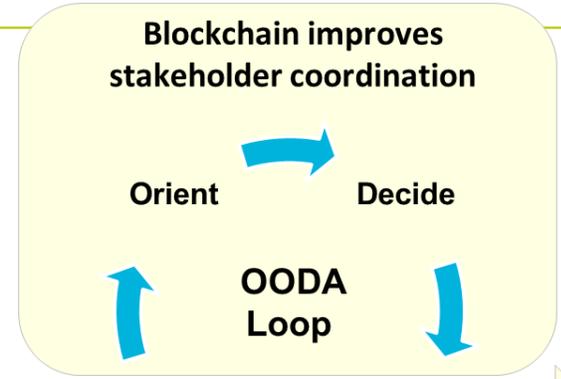
Blockchain

Capture transactional data in real time

Improve situational awareness

Improve mission effectiveness

All blockchains must support an improvement to mission effectiveness

MITRE

Potential Government Use Cases

- **Potential use cases exemplify blockchain-enabled stakeholder coordination**

- **Sharing information**
  - Decentralized, autonomous collection of data into a permissioned blockchain vs. centralized hierarchical means of collection into disparate legacy systems
  - Improves decision cycle
- **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
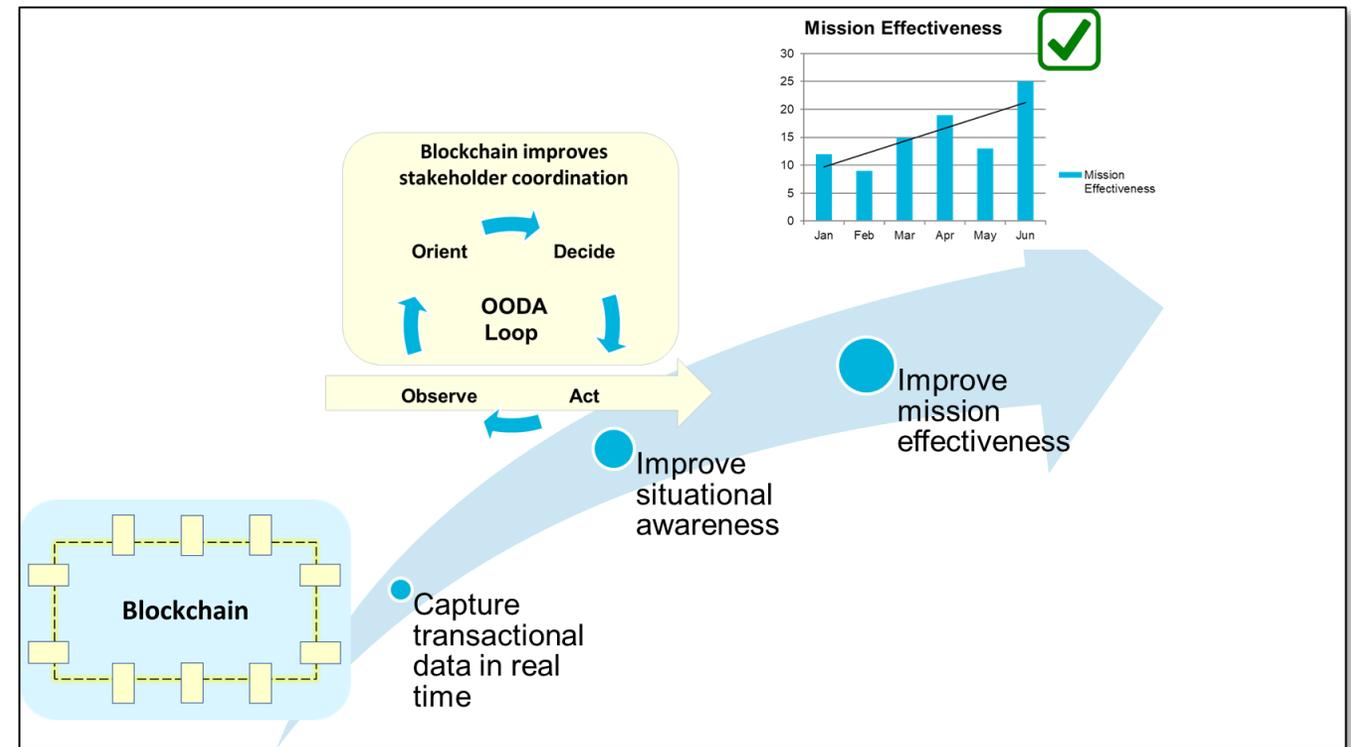
Govt Permissioned Blockchain Hypothesis

MITRE

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

- **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**

Blockchain

MITRE
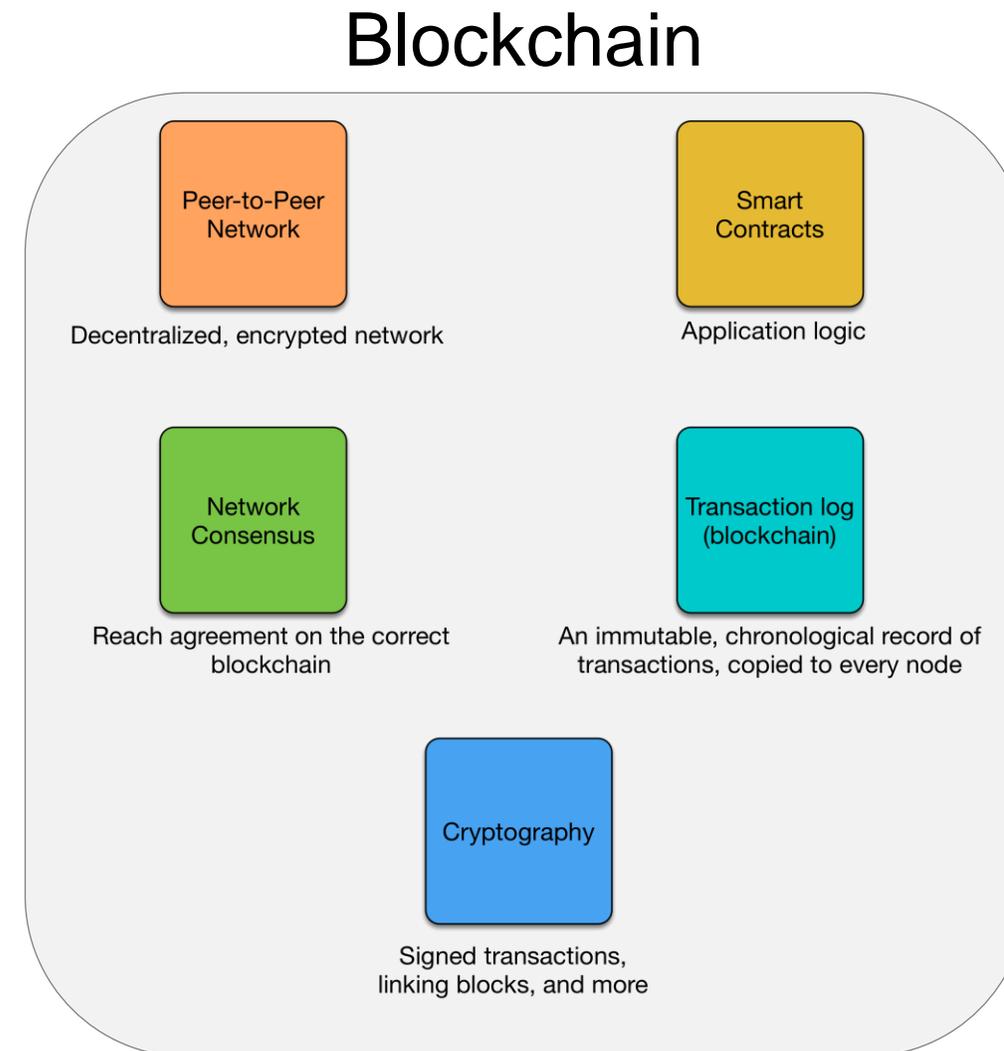
Operate a Permissioned Blockchain

- **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 orgs own and operate nodes as needed, per agreement**
- **Same orgs responsible for cyber maintenance (e.g. IAVAs)**
- **One or more orgs 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
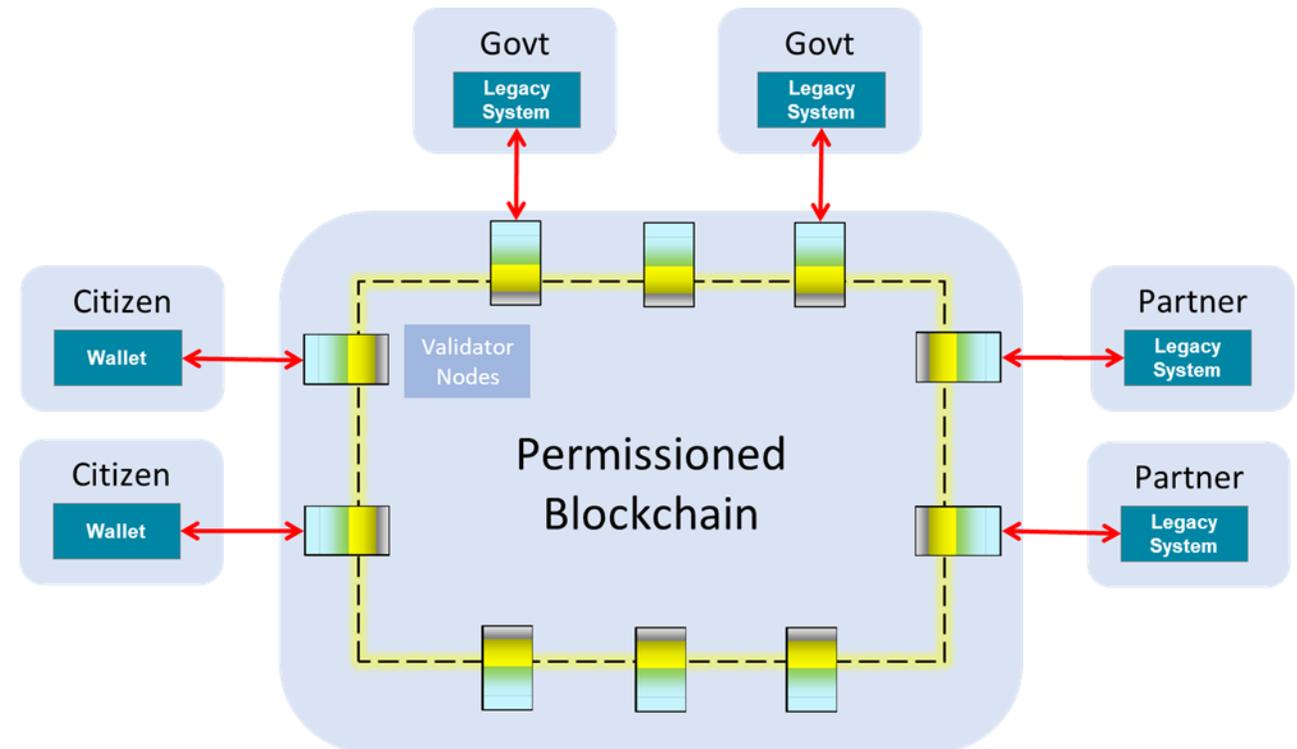
Blockchain Cost

Caveat: there is no handbook on costing blockchain (for now), will qualitatively apportion cost and magnitude below

**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.

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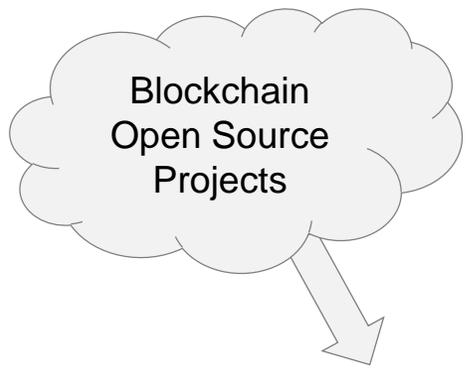
Incorporate blockchain in capability: Wrapping blockchain with interfaces, new processes, reporting, etc.

Negotiate with stakeholders: Stakeholder agreement required for functionality, operation, and sustainment
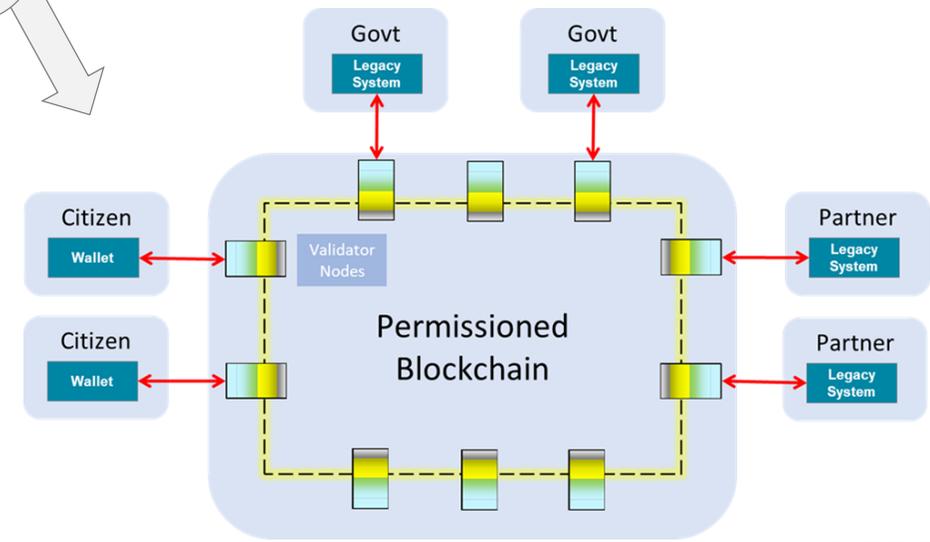
Cost Elements (2 of 3)
Detail

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
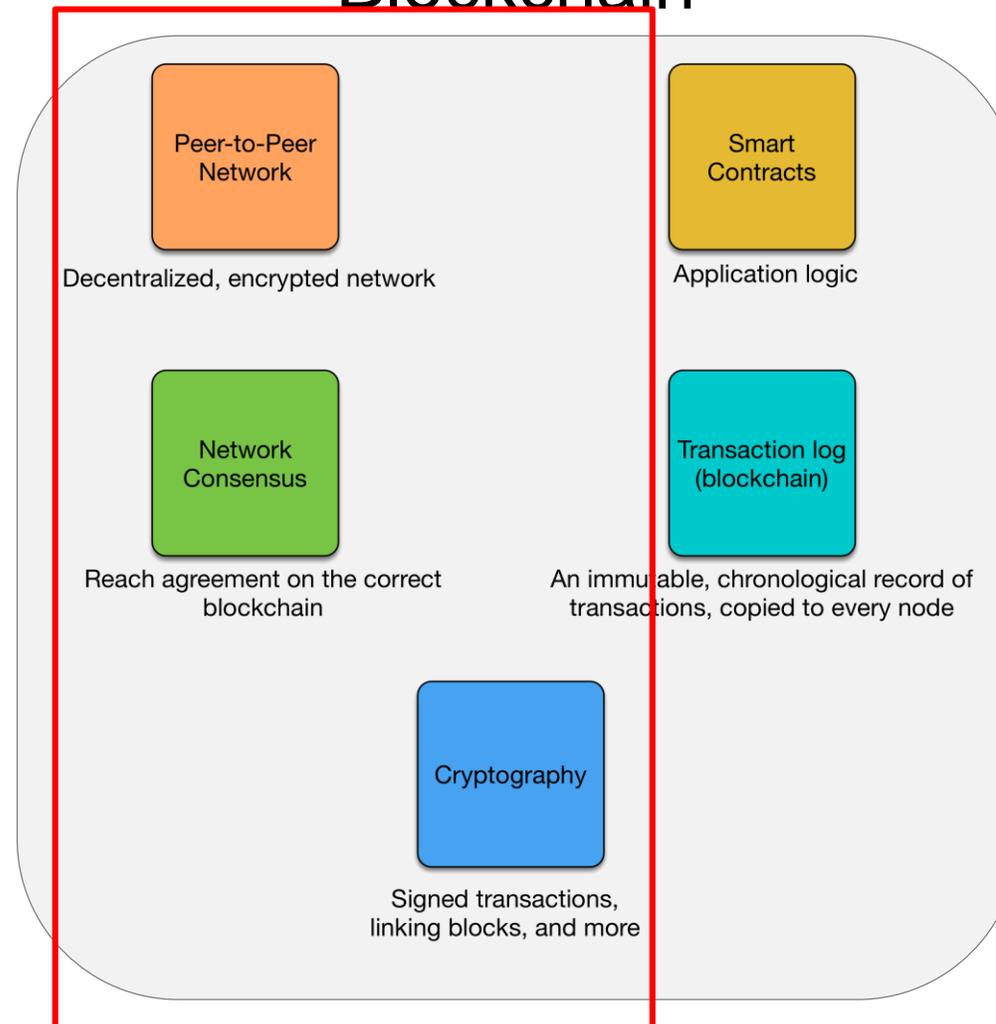
Cost Elements (3 of 3)
Detail

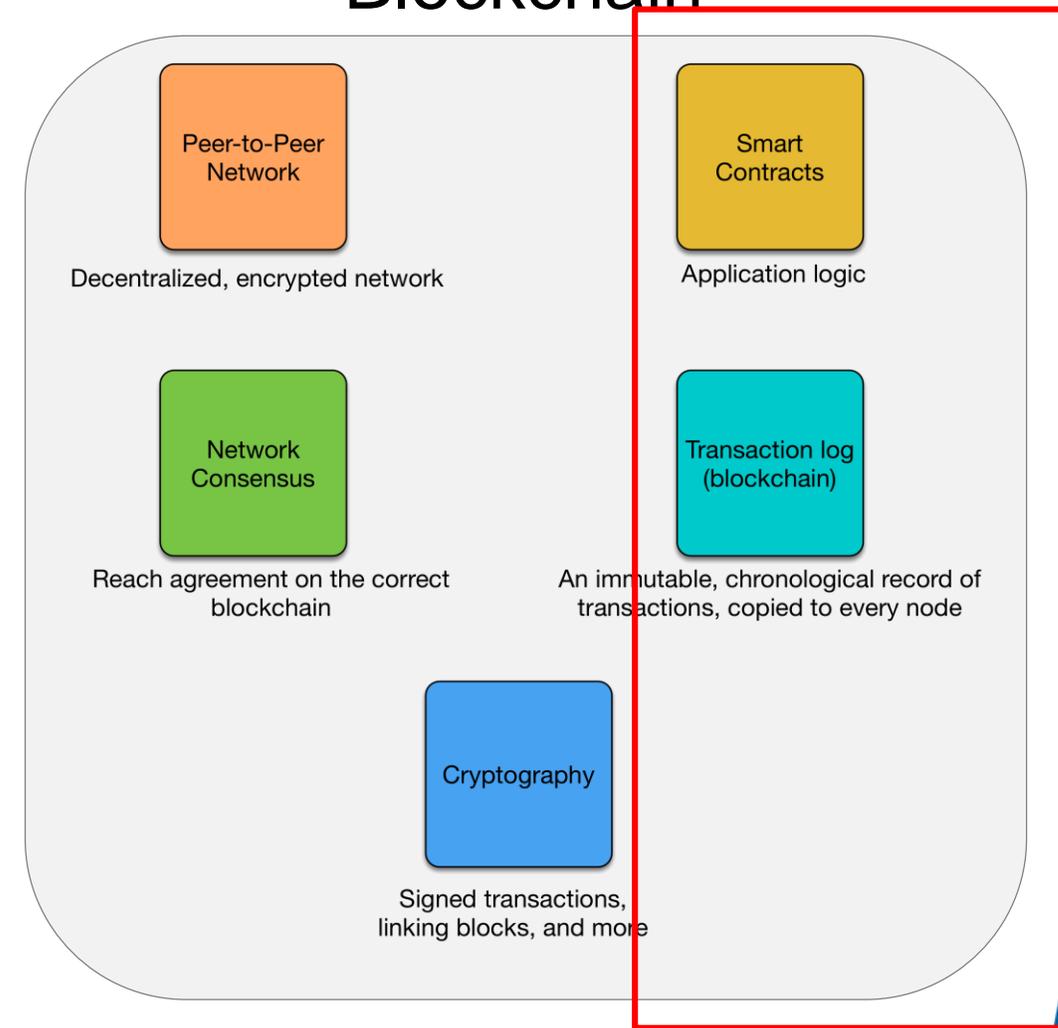| Component	Cost Element
Application logic	**Large item:** Smart contracts execute in blockchain and requires extensive design and testing. Blockchain transactions are final. Additional application logic (executes outside of blockchain) works with smart contracts, and constitutes new processes (see OODA 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.

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

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
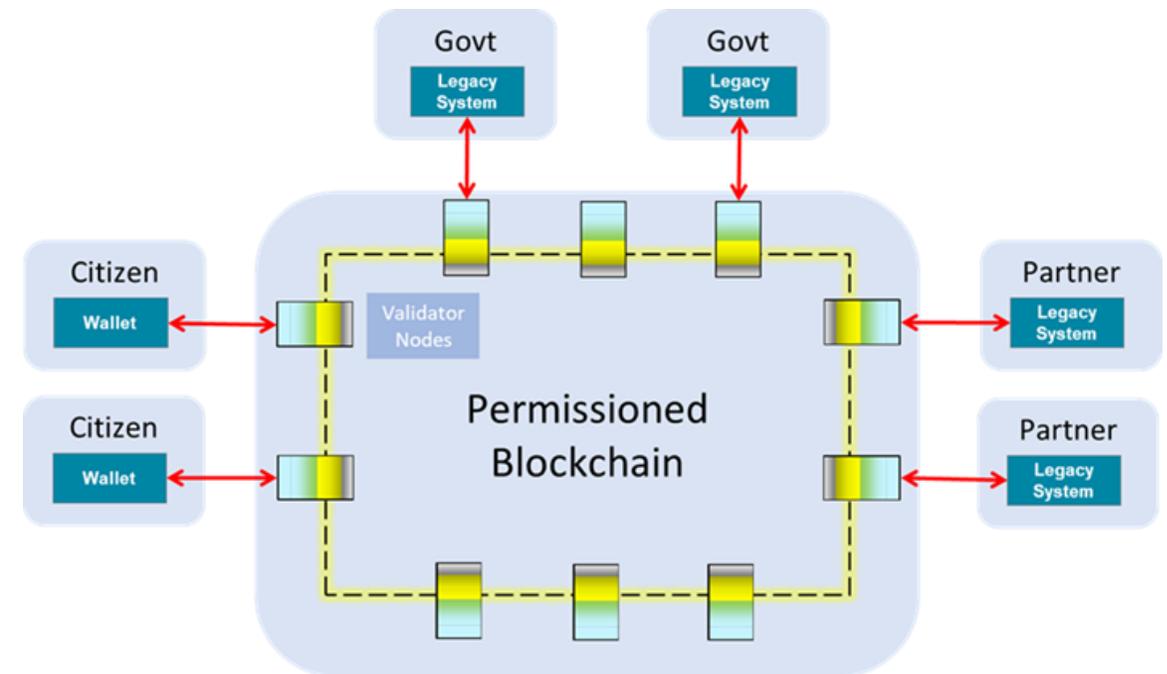
Cost Drivers

- **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

Cost Drivers

- **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
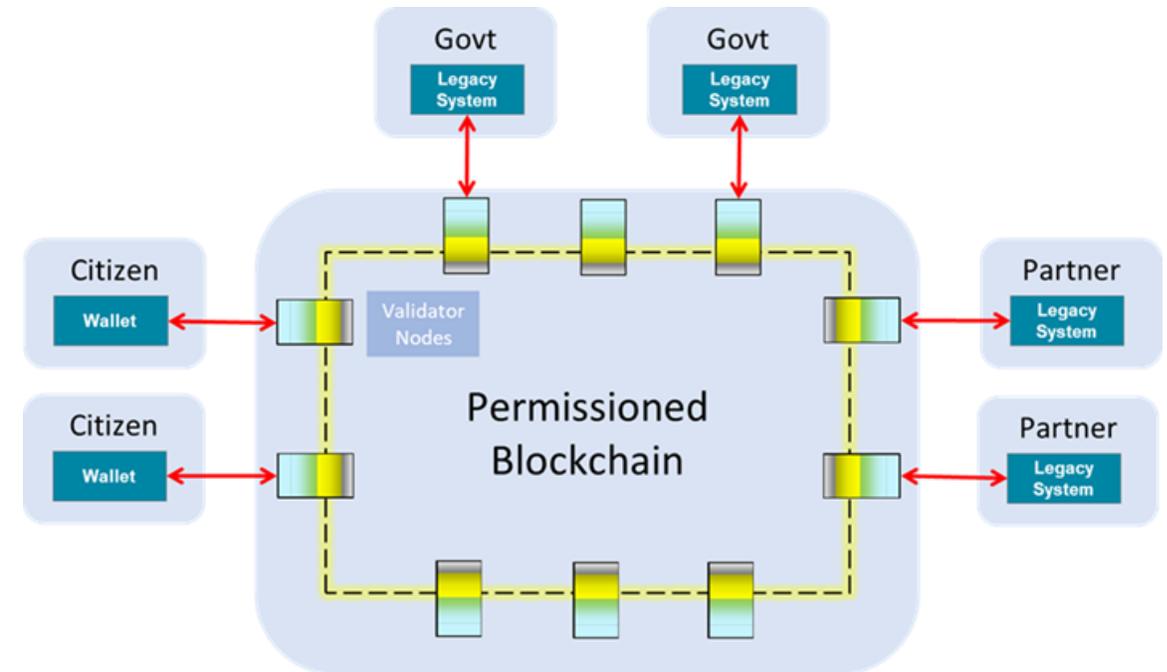
Cost Drivers

- **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
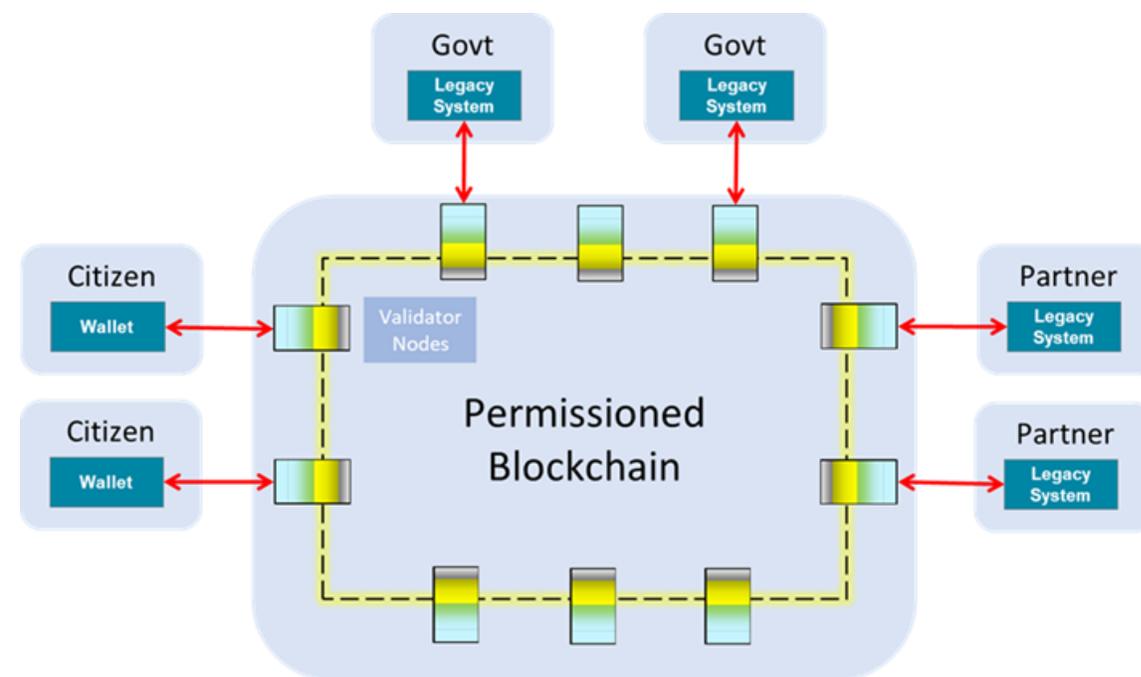
Cost Drivers

- **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

Cost Downstream

- ■ **Downstream 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

GOVT Legacy Systems

Downstream Impacts

GOVT Blockchain Node

Permissioned Blockchain

MITRE
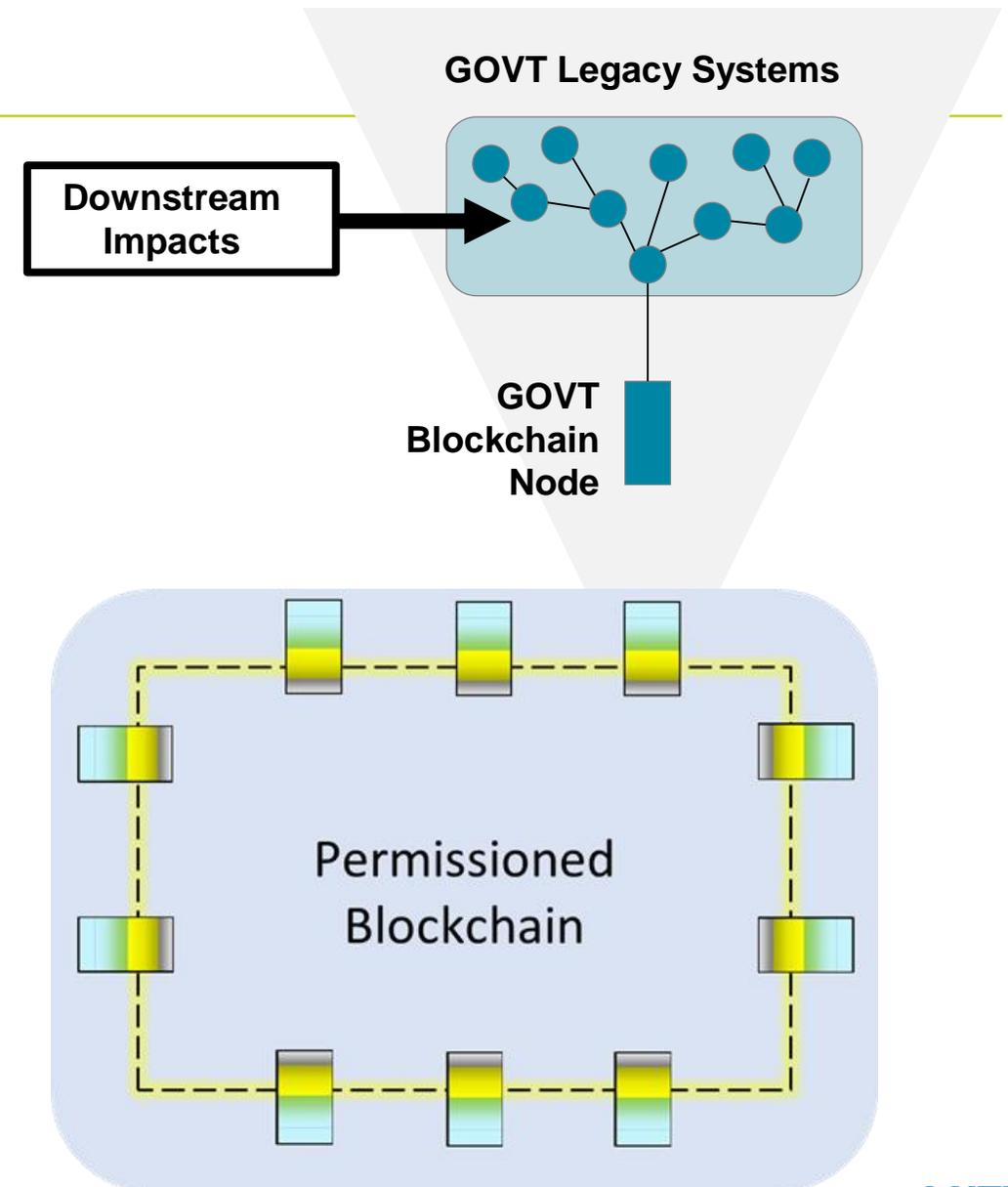
Summary Costing

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

Blockchain Components

GOVT Legacy Systems

Downstream Impacts

GOVT Blockchain Node

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

Blockchain Node

Blockchain software, AI, hardware

Permissioned Blockchain

MITRE

Open Cost 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

Discussion

POC

Harvey Reed
Blockchain Capability Lead

MITRE
hreed@mitre.org
781-439-7666 (mobile)

MITRE

BACKUP

MITRE

Blockchain Commercial Project (circa 2018)
Global Food Safety

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

- **Wal-Mart, 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

Wal-Mart: 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 Mearsk's blockchain enabled platform

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

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: Inter-bank transfers

https://www.swift.com/

MITRE