Beyond Blockchain Basics

Lessons Learned and Next Steps
from 3+ Years of R&D and Implementations

Homeland Security
Science and Technology

Anil John
Technical Director

DHS S&T's 3+ Years of R&D Investments … … to Understand Blockchain's Relevance to HSE

Security and Privacy

- Confidentiality, Integrity, Availability …
- Pseudonymous Operations, Selective Disclosure …

Integration Approaches & Gain/Pain

- Data Sharing Implications, On Chain vs. Off-Chain
- Storage of Information vs. Validation of Information

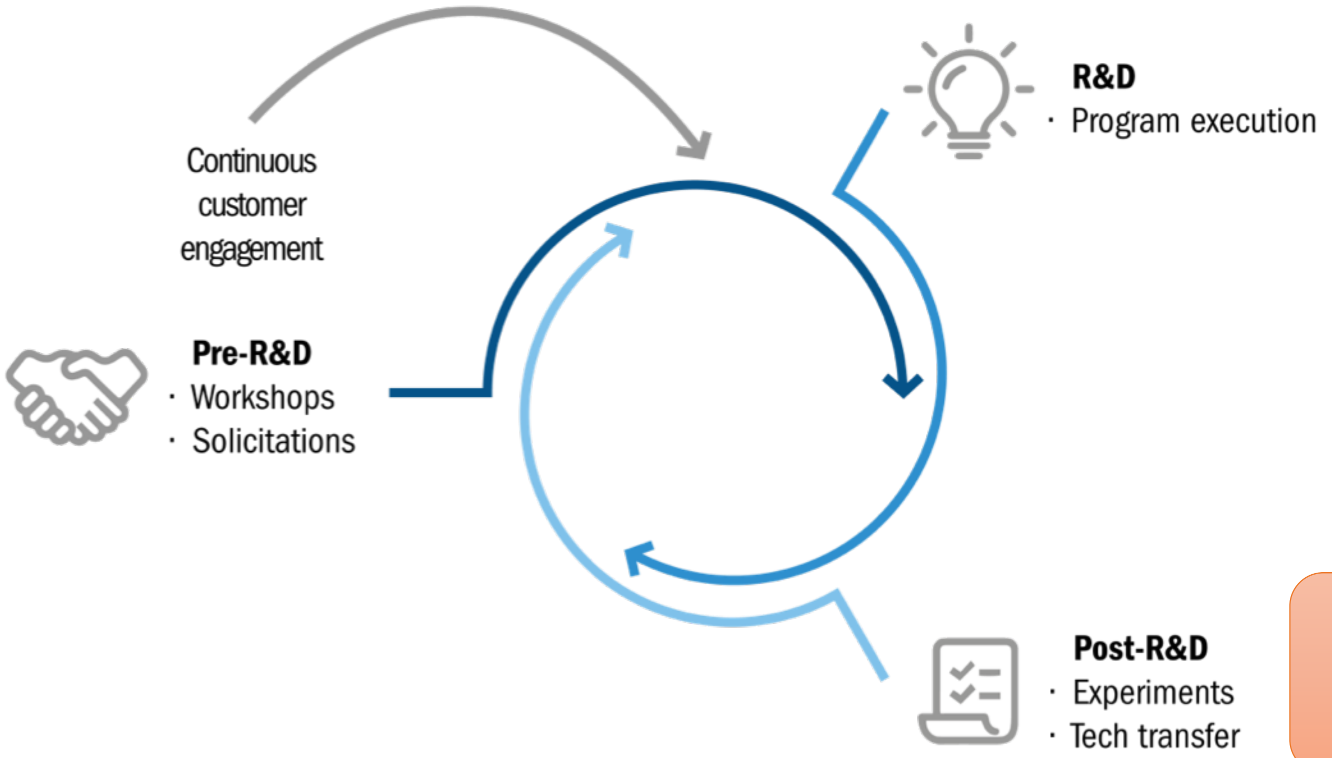
Digital Currency Forensics

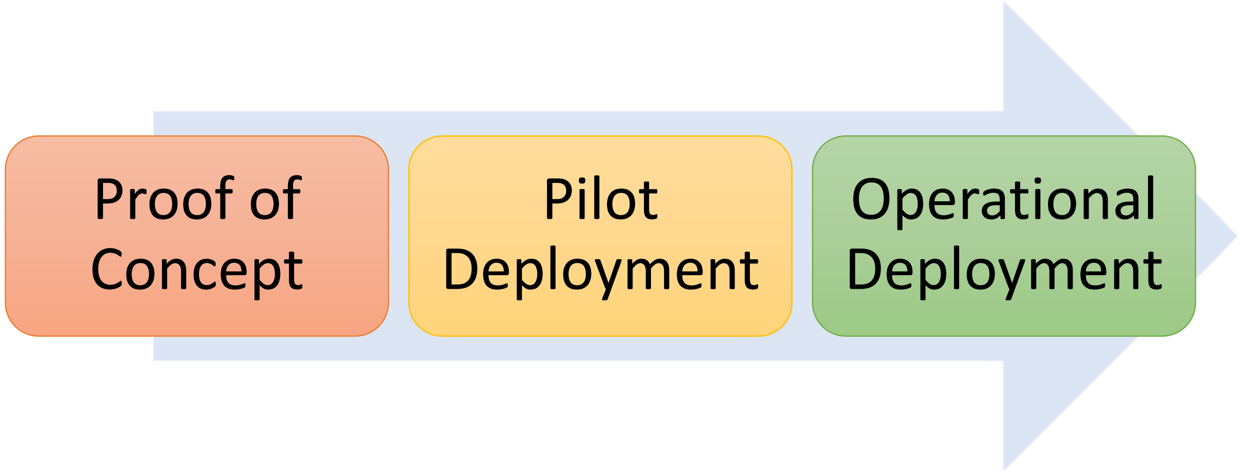
- Anonymous Currencies
- Anonymous Networks

DHS S&T R&D Programs
• Celerity Government Solutions, LLC • Digital Bazaar, Inc. • Narf Industries, LLC • Respect Network Corporation > Evernym, Inc. • SecureKey Technologies, Inc.
DHS S&T Silicon Valley Innovation Program
• Factom, Inc.

…

R&D Execution Model to Support Potential DHS Blockchain Operational Deployments



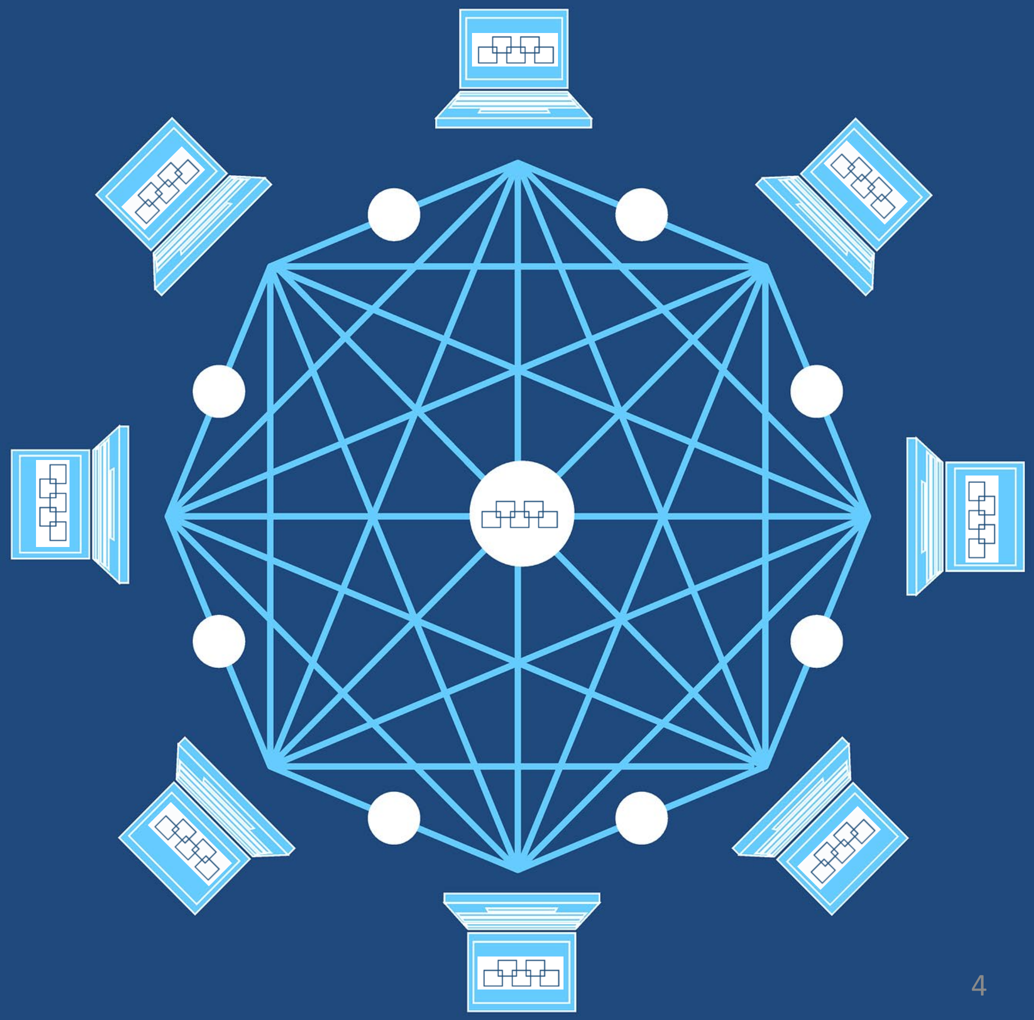


Lessons Learned from R&D Investments

Blockchain ≠ Blockchain ≠ Blockchain

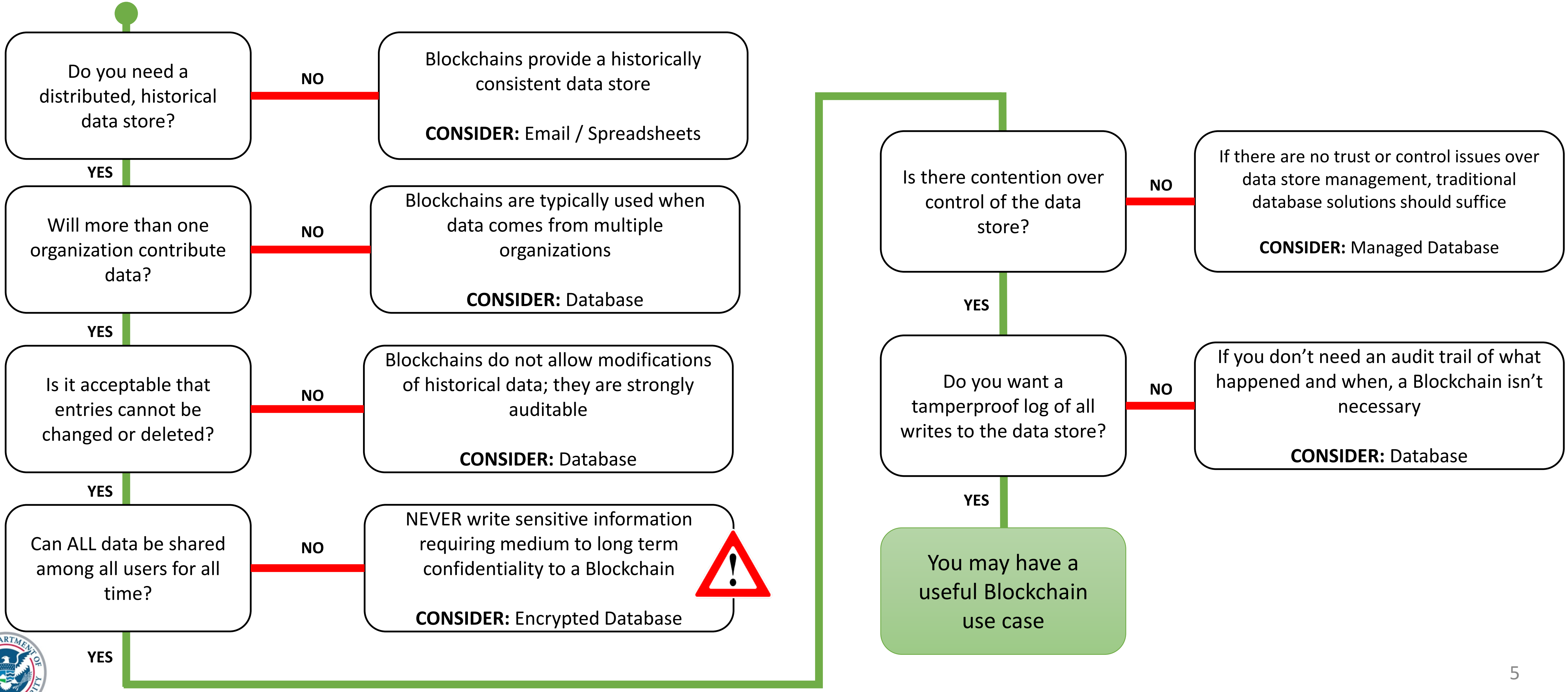
An authoritative book of records …

- With many copies that are kept synchronized
- In which multiple parties can create individual records
- Using consensus to determine the validity and order of written records
- Where each record is linked to the prior one
- Ensuring that written records cannot be modified or deleted without alerting the readers of the book



Lessons Learned from R&D Investments

Most Organizations Don’t Need A Blockchain



Lessons Learned from R&D Investments
No Common Set of Security & Privacy Defaults

Many Different Types of Distributed Ledgers (Blockchains) – Security & Privacy

Principle	Bitcoin	Ethereum	Stellar	IPFS	Blockstack	Hashgraph
Confidentiality	None	None	None	Hash-based content addresses	None	None
Information Availability	Block Mirroring	Block Mirroring	Ledger Mirroring	Graph and file Mirroring	Block Mirroring / DHT Mirroring	Hashgraph Mirroring; optional event history
Integrity	Multiple block verifications	Multiple block verifications	Latest block verification	Hash-based content addressing	Multiple block verifications	Consensus with probability one
Non-repudiation	Digital signatures	Digital signatures	Digital signatures	Digital signatures	Digital signatures	Digital signatures
Provenance	Transaction inputs/outputs	Ethereum state machine and transition functions	Digitally signed ledger transition instructions	Digital signatures and versioning	Transaction inputs & outputs and virtualchain references	Hashgraph Mirroring; optional event history
Pseudonymity	Public keys	Public keys and contract addresses	Public keys	Public keys	Public keys, but public information encouraged	Not supported; could be layered
Selective Disclosure	None	None	None	None	Selective access to encrypted storage	Not supported; could be layered

- Research results from S&T funded R&D conducted in 2016 by Digital Bazaar

Lessons Learned from R&D Investments

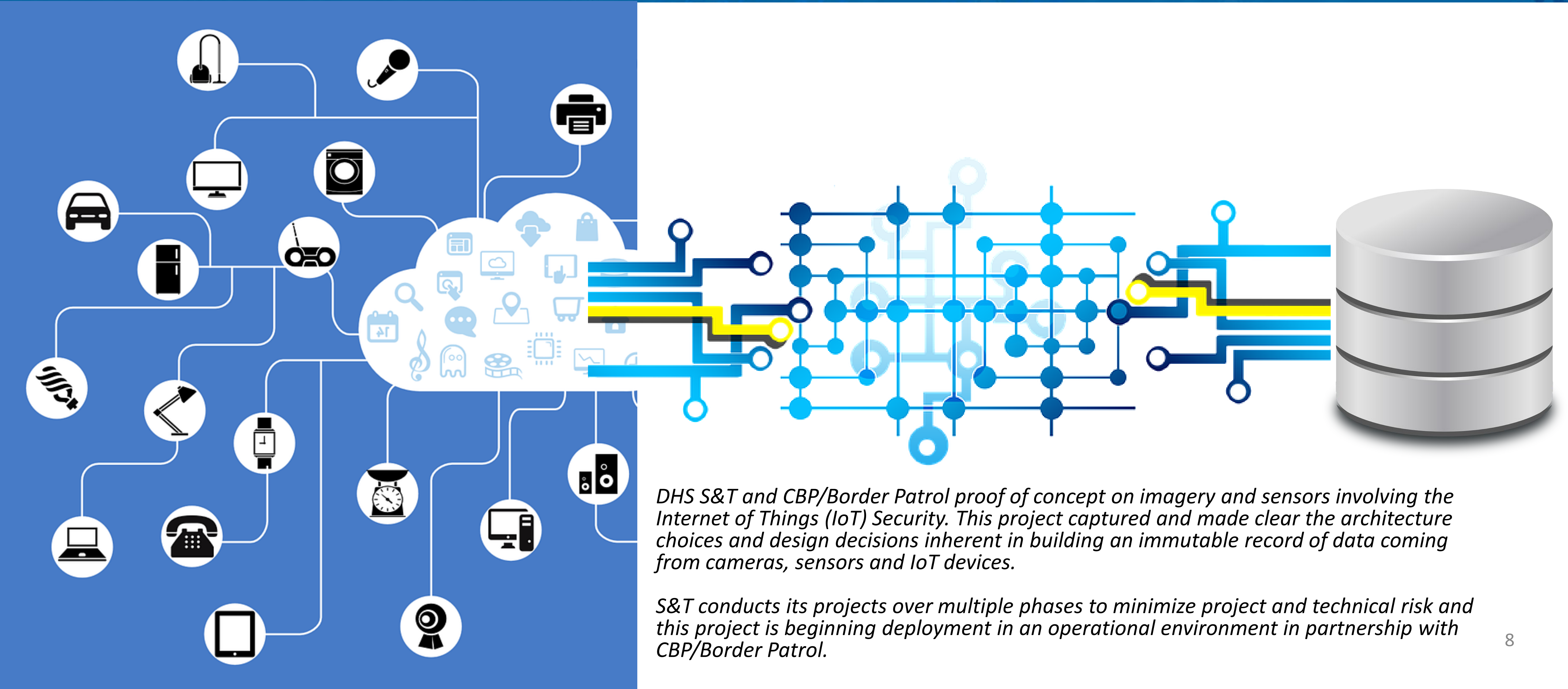
Varying Degrees of Performance

Many Different Types of Distributed Ledgers (Blockchains) – Performance

Principle	Bitcoin	Ethereum	Stellar	IPFS	Blockstack	Hashgraph
Consistency	Block verifications. 30-60 minutes	Block verifications. 20-60 minutes	Single block verification. Less than 1 minute	P2P mirroring. Limited primarily by network I/O. Several seconds for files less than 128KB.	Block verifications. 30-60 minutes	Consensus with probability one; Byzantine agreement, but attackers must control less than one-third
System Availability	Block verifications. 30-60 minutes	Block verifications. 20-60 minutes	Single block verification. Less than 1 minute.	Single storage request response. Several seconds for files less than 128KB	Block verifications. 30-60 minutes	Virtual voting; DoS resistant w/o proof-of-work, fast gossip
Failure Tolerance	Longest chain wins	Longest chain wins	Last balloted block always has consensus.	Content address hash. Highly resilient against network partitioning	Longest chain wins	Strong Byzantine fault tolerance
Scalability	Block size. 7 transactions per second	Block size. 7-20 transactions per second	Thousands to tens of thousands of transactions per second.	Thousands to tens of thousands of transactions per second. Scales linearly as nodes are added.	Block size. 7 transactions per second	Thousands to tens of thousands of transactions per second. Limited by bandwidth only
Latency	Block verifications. 30-60 minutes	Block verifications. 20-60 minutes	Single block verification. Less than 1 minute.	Single storage request response. Several seconds for files less than 128KB.	Block verifications. 30-60 minutes	Virtual voting; limited only by exponentially fast gossip protocol
Auditability	Full	Full	Full	Difficult	Full	Configurable
Liveliness	Full	Full	Full	Fails if nodes storing data fail	Full	Full
Denial of Service Resistance	Spend Bitcoin	Spend Ether	Spend Stellar	Files are only mirrored if requested	Spend Bitcoin	Signed State / Proof-of-stake / < 1/3 attackers
System Complexity	Medium	High	Medium	Medium	Medium High	Low, but not full system

- Research results from S&T funded R&D conducted in 2016 by Digital Bazaar

POC: Immutable Logging to Ensure Resiliency, Integrity and Independent Validation of IoT Device and Sensor Data



DHS S&T and CBP/Border Patrol proof of concept on imagery and sensors involving the Internet of Things (IoT) Security. This project captured and made clear the architecture choices and design decisions inherent in building an immutable record of data coming from cameras, sensors and IoT devices.

S&T conducts its projects over multiple phases to minimize project and technical risk and this project is beginning deployment in an operational environment in partnership with CBP/Border Patrol.

POC: Streamlining and Enhancing International Trade Facilitation via Free Trade Agreements

- Negotiated exchange of goods sanctioned by participating countries for improved trade
- Cumbersome paper process done in a post audit world where some participants have automation
- What are we testing?
  - Interoperability specifications
  - Segregated/Hybrid approach to Blockchain data
  - Safeguarding data against corporate breach, but utilizing Blockchain for generic data and status
  - Advancements over paper and automation processes
- POC Assessment Goals for DHS CBP and S&T
  - Legal
  - Policy
  - Technical

Lessons Learned/Validated by POC Implementations

If You Do Need A Blockchain, Be Aware …

- **Permissioned and private distributed ledger technologies** may be more suitable for leveraging existing business relationships and regulatory frameworks which are the majority of USG use cases
- **Architecture and design** cannot be hand-waved away (but often is in the race for market share!)
    - Integration points with existing environments
    - What is stored on-chain vs. off-chain? **Public on-chain pointers to private off-chain data stores?**
    - Private ledgers that can be anchored in public blockchains?
- There is no one-size-fits-all **ledger data format**, and standards for how to create the “data payload” that is written to a ledger are critical to interoperability across Blockchain implementations
- **Distributed key management** is not a solved problem, but needs to be for scalable deployment
- Immutability of records combined with encryption as a privacy tool is gated by the reality that **encryption has a time to live** which will eventually run out; this has real privacy and design implications
- **Smart contracts are relatively immature** and the contract execution environment must balance the security needs of the node with providing a richer (more error-prone) language

Enabling a Competitive, Diverse and Interoperable Blockchain / DLT Marketplace

- Funding, Championing and Using Globally Interoperable Standards and Specifications (pre-cursor to Standards)
- Investing in Customer Driven Proof-of-Concepts to Identify Integration Points and Gain/Pain Ratio
- Addressing Discovered Challenges

Championing Globally Interoperable Specifications
Decentralized Identifiers

- Globally Unique Identifier without the need for a central registration authority
  - Immutable
    - Identifier is permanent
  - Resolvable
    - Identifier can be looked up to identify metadata about entity it identifies
  - Cryptographically Verifiable
    - Identifier's ownership can be established and verified using public/private cryptographic keys

Decentralized Identifiers (DIDs) v0.10

W3C

Data Model and Syntaxes for Decentralized Identifiers (DIDs)

Draft Community Group Report 31 May 2018

Latest editor's draft:
https://w3c-ccg.github.io/did-spec/

Editors:
Drummond Reed (Evernym)
Manu Sporny (Digital Bazaar)

Authors:
Drummond Reed (Evernym)
Manu Sporny (Digital Bazaar)
Dave Longley (Digital Bazaar)
Christopher Allen (Blockstream)
Ryan Grant
Markus Sabadello (Danube Tech)

Participate:
GitHub w3c-ccg/did-spec
File a bug
Commit history
Pull requests

Abstract

Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority. DIDs are URLs that relate a DID subject to means for trustable interactions with that subject. DIDs resolve to DID Documents — simple documents that describe how to use that specific DID. Each DID Document contains at least three things: cryptographic material, authentication suites, and service endpoints. Cryptographic material combined with authentication suites provide a set of mechanisms to authenticate as the DID subject (e.g. public keys, pseudonymous biometric protocols, etc.). Service endpoints enable trusted interactions with the DID subject.

This document specifies a common data model, format, and operations that all DIDs support.

Championing Globally Interoperable Specifications

Verifiable Credentials

- Interoperability across issuers, holders and verifiers
  - Standardization of data formats
  - Standardization of digital signature schemes
- Digital version of physical credentials/attestations
  - Driver's Licenses
  - Passports
  - Training Certificates
  - Educational Certificates
  - …

Verifiable Credentials Data Model 1.0

Expressing verifiable information on the Web

W3C

W3C Editor's Draft 13 June 2018

This version:
https://w3c.github.io/vc-data-model/

Latest published version:
https://www.w3.org/TR/vc-data-model/

Latest editor's draft:
https://w3c.github.io/vc-data-model/

Editors:
Manu Sporny (Digital Bazaar)
Daniel C. Burnett (Invited Expert)
Dave Longley (Digital Bazaar)
Gregg Kellogg (Spec-Ops)

Authors:
Manu Sporny (Digital Bazaar)
Dave Longley (Digital Bazaar)

Participate:
GitHub w3c/vc-data-model
File a bug
Commit history
Pull requests

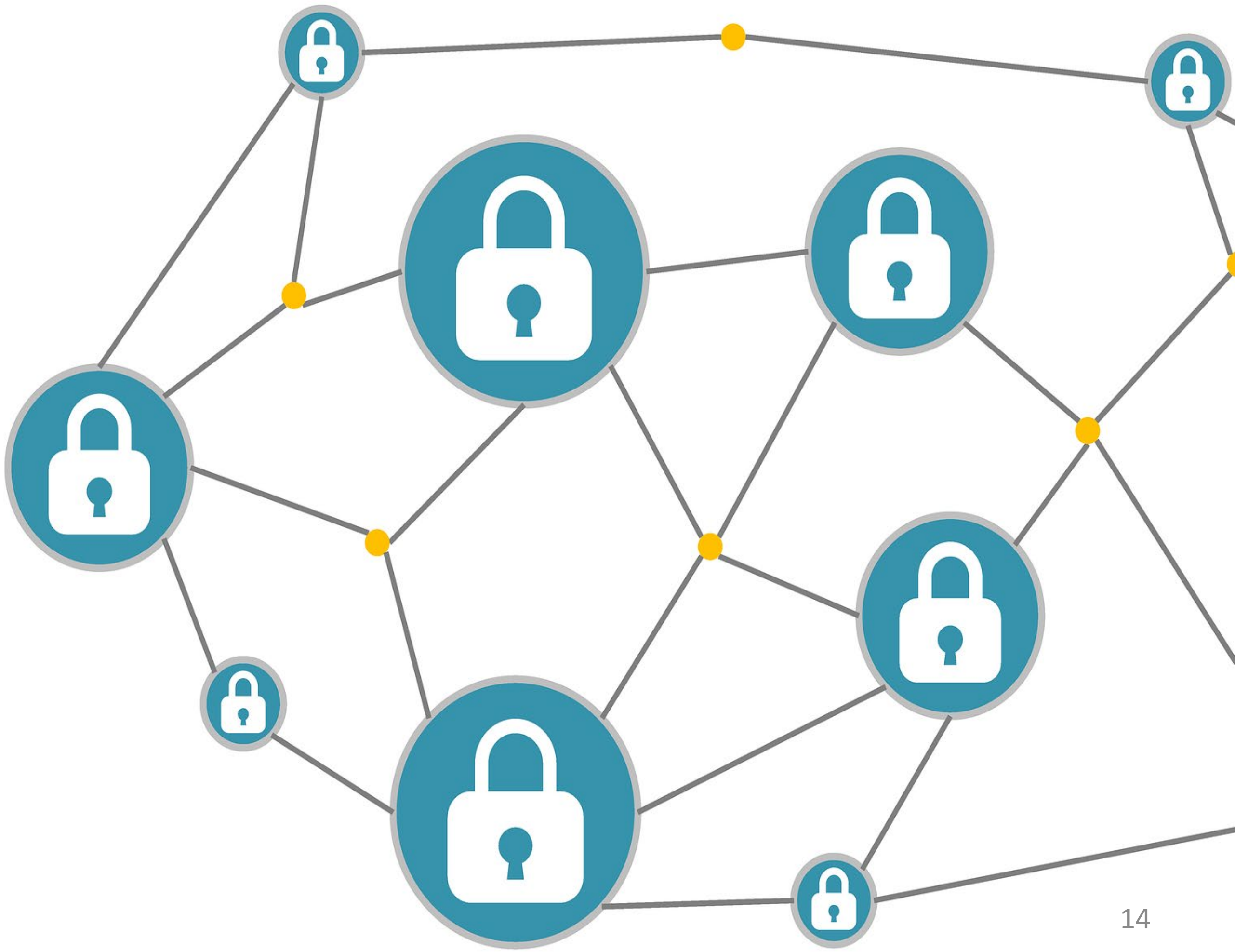
Abstract

Credentials are a part of our daily lives; driver's licenses are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable holders to travel between countries. This specification provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable.

Championing Globally Interoperable Specifications

Multi-Party Distributed Key Management

- Tackling the hard challenge of distributed key management
  - Provisioning
  - Revocation
  - Re-Issuance
- Supports Cross-Enterprise Managed Deployments
- Using *NIST Special Publication 800-130: A Framework for Cryptographic Key Management Systems* as a starting point
- Potential Path to Standardization - TBD



CBP Adoption of S&T Championed Blockchain Interoperability Specifications as a US Customs Standard

U.S. Customs and Border Protection

AUG 0 8 2018

MEMORANDUM FOR: John P. Sanders
Chief Operating Officer

FROM: Brenda B. Smith
Executive Assistant Commissioner
Office of Trade

Kathryn Kolbe
Executive Assistant Commissioner
Enterprise Services

Phil Landfried
Assistant Commissioner
Office of Information and Technology

SUBJECT: Setting Standards for Blockchain/Distributed Ledger Technology

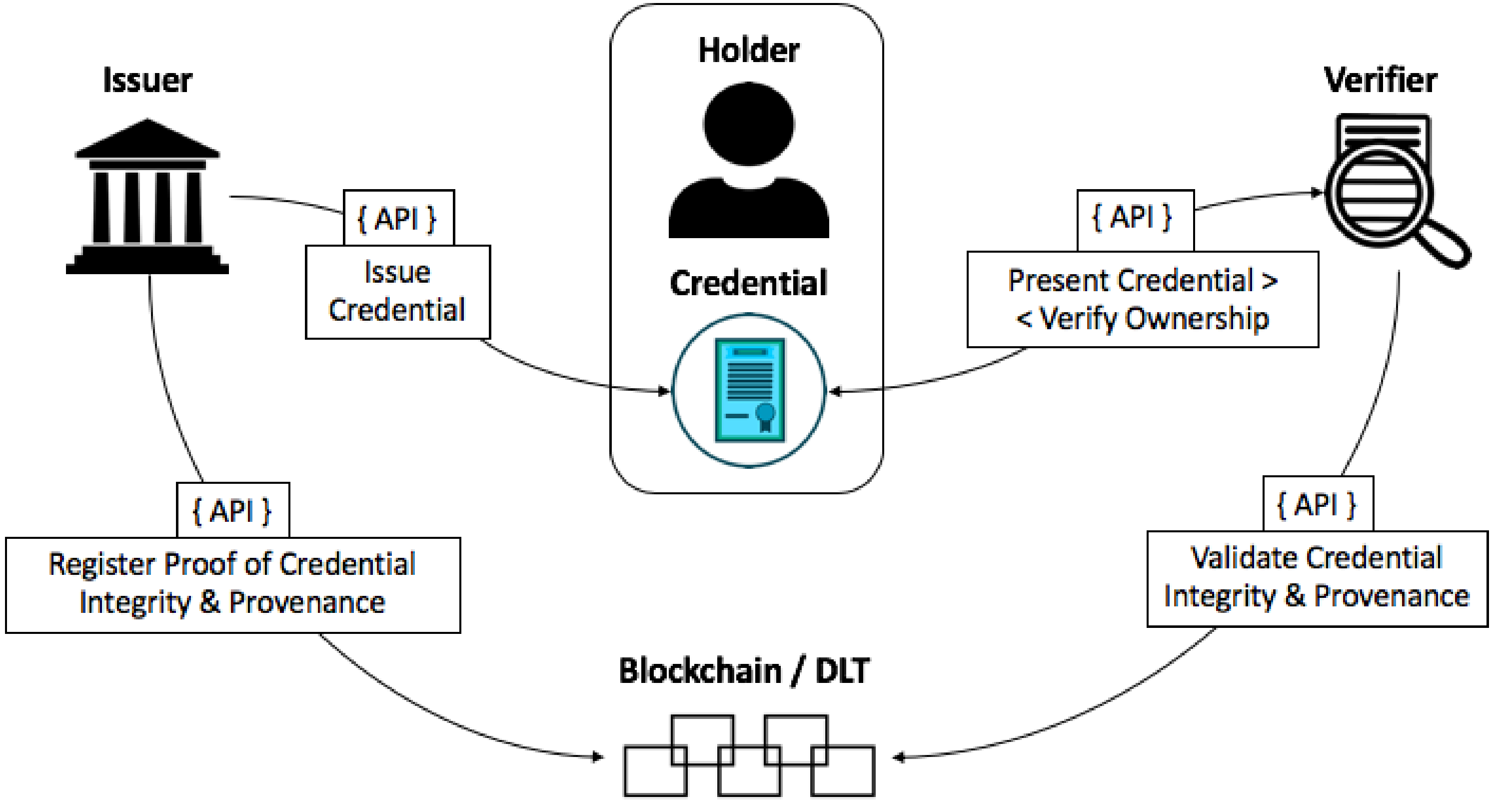
DHS S&T has invested over three years of time, money, and effort into researching the specifications necessary to allow multiple blockchains to interact with each other. Interoperability allows the government to remain impartial toward which blockchain software is utilized by our trade partners and removes the need for CBP to continuously build customized Application Program Interfaces to communicate with users of other technology.

Proposed Path Forward:
The Office of Trade (OT) and the Office of Information and Technology (OIT) jointly recommend that:

1. CBP adopt the specifications developed and championed by DHS S&T as a CBP standard.
2. OT and OIT jointly engage other U.S. Government stakeholders, such as the DHS Chief Information Officer (CIO), the White House CIO Council, and others, to push for broader adoption of these standards and to develop an effective "whole of government" approach towards this use-case of blockchain technology.

Challenge: Mitigating Forgery & Counterfeiting of Official Licenses & Certificates

- Person-ownership of verifiable claims and certificates
- Selective disclosure of claim information with the Person's consent
- Pluralism of operators and technologies
- Support for online and off-line presentation of claim
- Non-CRL based revocation methods (Issuer initiated, Person initiated and/or Multi-sig based) that removes issuer dependency
- Very high resistance to data deletion, modification, masking or tampering



DHS S&T Silicon Valley Innovation Program

Preventing Forgery & Counterfeiting of Licenses & Certificates

Preventing Forgery & Counterfeiting of Certificates and Licenses

SVIP Call # 70RSAT19R00000002

Application Deadline (1st): 11 Jan, 2019

Register Now to Attend Industry Day
11 Dec, 2018 @ Menlo Park, CA, USA

- DHS Operational Components (CBP, TSA, USCIS etc.) need to issue, validate and verify entitlements, attestations and certificates
  - Travel
  - Citizenship and Immigration Status
  - Employment Eligibility
  - More …
- Current issuance processes are paper based, non-interoperable and susceptible to loss, destruction, forgery, and counterfeiting
- Seeking digital solutions for:
  - Issuance, Validation and Verification of Certificates, Licenses and Attestations
  - Storage and Management of Certificates, Licenses and Attestations
  - Consolidating Decentralized and Derived PIV Credentials

https://go.usa.gov/xPGsr

Conclusions and Considerations

- Potential for the development of “walled gardens” or closed technology platforms that do not support common standards for security, privacy, and data exchange
- Interoperability requires addressing architecture, protocol, payload and policy aspects of any solution
  - Need investments in globally interoperable standards
  - Standards must be informed by lessons learned from business driven proof of concepts
- Rip-n-Replace is NOT a successful path to Enterprise Integration
  - Thoughtful, creative, system architectures and design play crucial roles when it comes to meeting the Gain to Pain ratio threshold of any Enterprise adoption
  - Data privacy continues to be a critical component of any distributed solution
  - Customer driven Proof of Concept implementations are in process to determine if the technology gains outweigh the process change & integration pain necessary for adoption
- Interoperable Decentralized Identifiers, Data Exchange Standards & Distributed key management are not solved problems
  - These have both technology and standards components that need to be addressed
  - Scalable deployment needs solution diversity to prevent vendor tech lock-in

DHS S&T is making targeted R&D investments to close the above identified capability gaps.
We look forward to collaborating with other stakeholders who have shared interests!

Homeland Security

Science and Technology

Anil John

Technical Director
Silicon Valley Innovation Program

anil.john@hq.dhs.gov