Beyond Blockchain Basics

Lessons Learned and Next Steps from 3+ Years of R&D and Implementations
DHS S&T’s 3+ Years of R&D Investments …
… to Understand Blockchain’s Relevance to HSE

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.

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

- Continuous customer engagement
- Pre-R&D: Workshops, Solicitations
- R&D: Program execution
- Post-R&D: Experiments, Tech transfer
- Proof of Concept
- Pilot Deployment
- Operational Deployment
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
Blockchain ≠ Blockchain ≠ Blockchain
Lessons Learned from R&D Investments
Most Organizations Don’t Need A Blockchain

- Do you need a distributed, historical data store?
  - YES
  - NO
  - Blockchains provide a historically consistent data store
    - CONSIDER: Email / Spreadsheets

- Will more than one organization contribute data?
  - YES
  - NO
  - Blockchains are typically used when data comes from multiple organizations
    - CONSIDER: Database

- Is it acceptable that entries cannot be changed or deleted?
  - YES
  - NO
  - Blockchains do not allow modifications of historical data; they are strongly auditable
    - CONSIDER: Database

- Can ALL data be shared among all users for all time?
  - YES
  - NO
  - NEVER write sensitive information requiring medium to long term confidentiality to a Blockchain
    - CONSIDER: Encrypted Database

- Is there contention over control of the data store?
  - YES
  - NO
  - If there are no trust or control issues over data store management, traditional database solutions should suffice
    - CONSIDER: Managed Database

- Do you want a tamperproof log of all writes to the data store?
  - YES
  - NO
  - If you don’t need an audit trail of what happened and when, a Blockchain isn’t necessary
    - CONSIDER: Database

- You may have a useful Blockchain use case
## Lessons Learned from R&D Investments

### No Common Set of Security & Privacy Defaults

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

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

- Research results from S&T funded R&D conducted in 2016 by Digital Bazaar
Many Different Types of Distributed Ledgers (Blockchains) – Performance

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

- 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
Data Model and Syntaxes for Decentralized Identifiers (DIDs)

Draft Community Group Report 31 May 2018

Latest editor’s draft:
https://w3c.org/did/draft-spec/

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

Authors:
Drummond Reed (Evernym)
Muni Sporny (Digital Bazaar)
Dave Longley (Digital Bazaar)
Christopher Allen (Blockstream)
Ryan Grant
Marius Sabadeiko (Danube Tech)

Participate:
GitHub w3c-org/did-spec
File a bug
Commit History
Pull requests

Copyright © 2018 the Contributors to the Decentralized Identifiers (DIDs) v0.10 Specification. Published by the W3C Community Group under the W3C Community Contributor License Agreement (CCA). A human-readable summary is available.

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 trustworthy 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
  - …
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

AUG 08 2018

MEMORANDUM FOR: John P. Sanders
Chief Operating Officer

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

Kathryn Kolb
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 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

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

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!