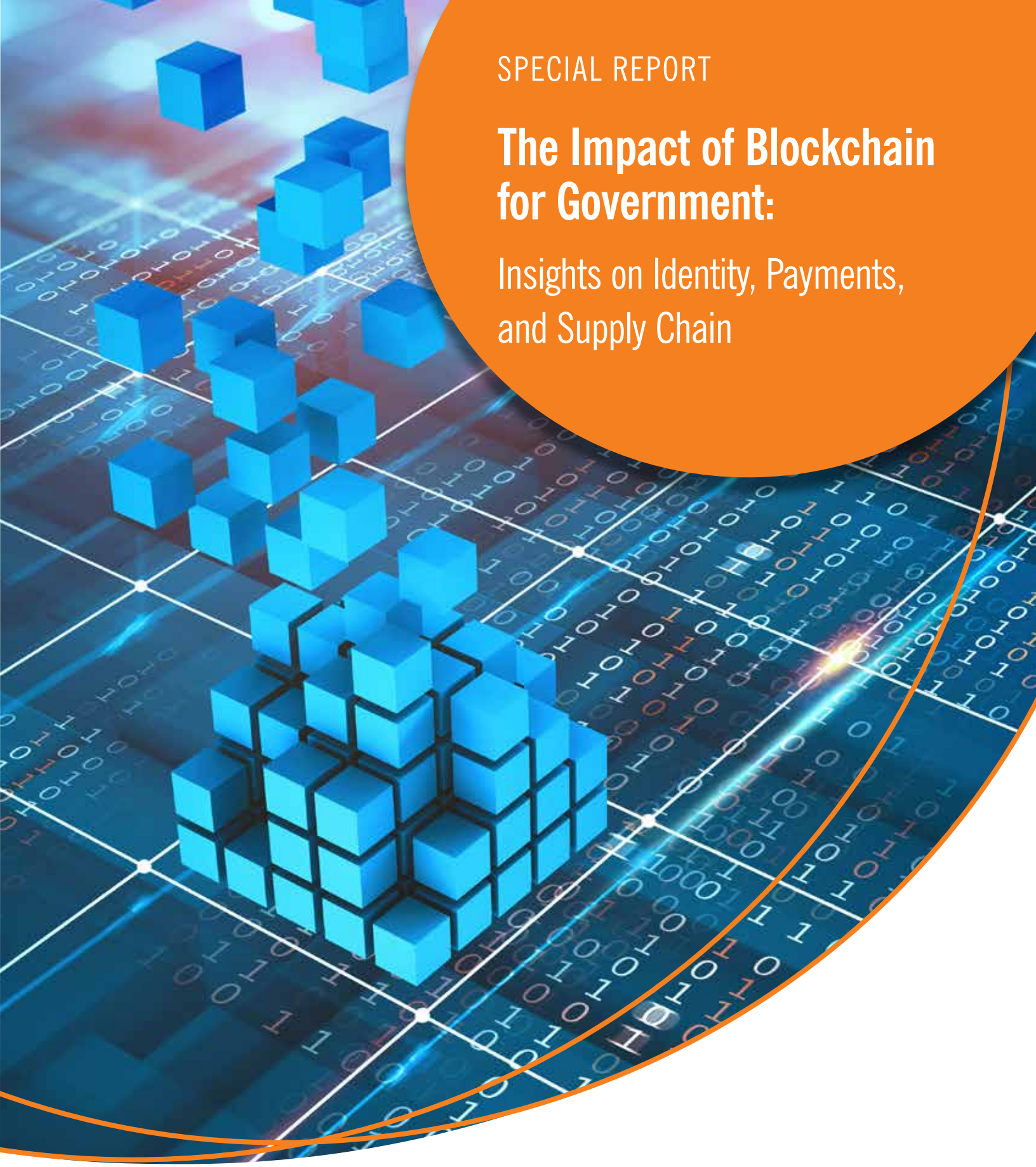


SPECIAL REPORT

The Impact of Blockchain for Government:

Insights on Identity, Payments, and Supply Chain

Thomas Hardjono
MIT Connection Science

MIT Connection Science

IBM Center for The Business of Government
20 years of research for government: informing today, envisioning tomorrow
1998-2018

The Impact of Blockchain for Government: Insights on Identity, Payments, and Supply Chain

Thomas Hardjono
MIT Connection Science

IBM Center for
The Business of Government
20 years of research for government:
informing today, envisioning tomorrow
1998-2018

TABLE OF CONTENTS

ABOUT THE AUTHOR

Dr Thomas Hardjono is the Director of the MIT Trust: Data Consortium, part of MIT Connection Science. Prior to this he was the Executive Director of the MIT Kerberos Consortium for over 5 years, championing the deployment of the MIT Kerberos protocol to several platforms and ecosystems, including IoT devices, Mobile platforms and Enterprise Cloud services. Thomas has held several industry key technical positions in the past, including Distinguished Engineer at Bay Networks, Principal Scientist at VeriSign PKI, and CTO roles at several start-ups. He has been at the forefront of several identity, trust and cybersecurity initiatives in industry, ranging from network multicast security, IoT Security, trusted computing to scalable identity systems, P2P networks and blockchain systems. Thomas has authored several technical papers, patents and books covering cryptography, networking, identity and blockchain security.

THOMAS HARDJONO

FOREWORD

On behalf of the IBM Center for The Business of Government, we are pleased to present this special report, *The Impact of Blockchain for Government: Insights on Identity, Payments, and Supply Chain,* by Thomas Hardjono with MIT Connection Science, in consultation with the Congressional Blockchain Caucus.

Business transactions take place every second—orders, payments, account tracking, and many more. Often, all participants to a transaction have their own ledgers—and, thus, their own individual versions of the facts. Having multiple ledgers can lead to error, fraud and inefficiencies—vulnerabilities that can be reduced by having a common view of a transaction end-to-end.

DANIEL J. CHENOK

Blockchain technology enables a shared ledger to record the history of transactions with consistency and certainty. In a blockchain network, all parties to a transaction must give consensus before a new transaction is added—and once recorded in the blockchain network, a transaction cannot be altered. Blockchain eliminates or reduces paper processes—speeding up transaction times, increasing efficiencies, and building trust among participants to a transaction.

How can blockchain benefit government? How can government lead the way to a broad-based blockchain evolution that drives economic vitality? In this report, Thomas Hardjono—Director of the MIT Trust: Data Consortium—addresses these and related challenges by drawing insight from three roundtable discussions in 2017-18 among key leaders and stakeholders, hosted by the Congressional Blockchain Caucus. The roundtables helped frame key issues impacting blockchain and government, particularly focused on how blockchain can improve identity management, payment accuracy, and supply chain integration.

PETE TEIGEN

We hope that this report provides timely insight on the potential for blockchain to help government, as agencies expand their implementation of this important technology in the years to come.

Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
chenokd@us.ibm.com

Pete Teigen
Government Solutions Center of Competence
Blockchain/Mobile/Emerging Tech
IBM Global Business Services
pete.teigen@us.ibm.com

EXECUTIVE SUMMARY

The emergence of blockchain technology—as the promise of the foundation for the next-generation global commerce infrastructure for frictionless transacting—has resulted in numerous countries placing greater emphasis on investing and innovating in this space.

Governments from several nations have developed mission and vision statements regarding distributed ledger technology, and have taken steps to reduce or remove regulatory hurdles for their technology industries.

Strong industry consensus exists around the belief that blockchain technology will be the leading edge of "next Internet" economy. It is imperative that government and industry work together to continue and strengthen technological and market leadership in this new area, and to address potential policy and regulatory incompatibility that may constrain growth of the emerging digital-blockchain economy.

To begin addressing these concerns through open dialog, the Congressional Blockchain Caucus, under the leadership of Congressmen David Schweikert (R-Arizona) and Jared Polis (D-Colorado), initiated and conducted three roundtable discussions with a broad cross section of government and industry representatives during 2017-2018. The following sections, further described in the associated appendices at the end of this report, summarize the roundtable's goals, the topics discussed, and the common themes that emerged from the input of the participants.

Roundtable Goals

The goals of these roundtable meetings follow.

- **Understand potential use of blockchains as an emerging technology:** Bring together government and industry leaders and experts to exchange knowledge, experiences, and expertise to deepen understanding of the true potential of blockchain technology.
- **Identify areas of common interest:** Obtain a shared understanding regarding the potential areas for the application of blockchain technology, both short- and long-term, which can transform certain industry sectors.
- **Accelerate adoption and deployments:** For certain areas of application, accelerate and expand the adoption of blockchain technology.
- **Identify existing gaps that impede implementations:** Understand the current state of the technology, including the gaps or barriers to full deployment.
- **Identify components being assessed across industries, businesses, and government agencies:** Share experiences, lessons learned, and future plans regarding components of blockchain technology that industries are examining for their own application, with a goal of encouraging cross-sector standardization for key aspects of distributed ledger technology.

Areas of Discussion

The three roundtables each focused on a key theme regarding blockchain's impact for government.

(1) **Digital identity:** The secure identity of entities (person, organization, government) and assets (including the Internet of things, devices, and tangible and intangible items of value) involved in transactions over a blockchain system is crucial for the trusted operations of the system, and for compliance with various requirements such as taxation. Identity and membership management solutions already exist and can be applied to private, permissioned blockchain systems; features within these solutions should be evaluated for system suitability.[1] Specifically, four steps can enable government to start in using blockchain to address identity challenges:

- Evaluate existing identity and membership management solutions to identify features for permissioned blockchain systems in the short term.
- Experiment with integrating these existing solutions with open source blockchain implementations.
- Create a roadmap with a two- to three-year horizon for identity and membership management approaches to smart contracts within permissioned blockchains.
- Develop a long-term plan with a five-year horizon to address identity and membership management for permissionless public blockchain systems. Use open source blockchain implementations to understand challenges in the identity space for permissionless blockchains.

See Appendix A for detailed notes of the identity roundtable discussion.

(2) **Payments:** Some current deployments of blockchain technology provide a promising foundation for a frictionless, more efficient, and low-cost payments and settlements mechanism. When combined with blockchain-based identity technology, the promise of payment fraud reduction becomes tangible, with more efficient means of conducting processes like Know Your Customer. Federal leaders and agencies with a mission to enable innovation could help reduce risk in the regulatory environment for companies wanting to experiment and innovate with blockchain technologies. Benefits obtained through this strategy include:

- Signaling to the market that innovation will not be punished.
- Encouraging the use of open development environments—often referred to as "sandboxes"—for collaborative innovation and accelerated solutions.
- Broader adoption of use cases and industry standards.[2]

See Appendix B for detailed notes of the payments roundtable discussion.

(3) **Supply chain and provenance:** The distributed nature of ledger components in a blockchain system offers greater end-to-end visibility into the shared-state of information among participants, and therefore provides a promising foundation for next-generation supply chain management infrastructures. Rethinking the supply chain paradigm for a blockchain context demonstrates that supply chain involves more than just moving and tracking a product from cradle to grave, but also involves seeing beyond the process from

1. http://businessofgovernment.org/blog/how-can-blockchain-technology-help-government-drive-economic-activity
2. http://www.businessofgovernment.org/blog/how-can-blockchain-technology-help-government-drive-economic-activity-0

component parts to finished goods. This transforms traditional supply chain analysis, expanding to understand the supply chain of ideas, supply chain of data, supply chain of identities, and supply chain of trust.[3]

See Appendix C for detailed notes of the supply chain roundtable discussion.

The participants in each roundtable meeting had little overlap—in other words, there were few repeat attendees. This approach was taken in order to gather input from key industry and government leaders in the specific topical area, and to include each sector and segment of industry and economy as broadly as possible.

Common Themes in Discussions

Across the three daylong roundtable meetings, a number of overarching common themes emerged, often recurring within a different meeting topic with different attendees. Three overarching common themes follow.

- **Leadership and vision from government:** Currently there is a need for greater vision and leadership across government regarding the development of technology for a digital-blockchain economy, and the U.S. role in this future economy. Industry leaders believe this technology will be core to the future of the economy as a whole, just as the Internet has become. This foundational economic impact may range from supply-chain logistics management, to finance and insurance, to identity, to government services, and more.
- **Close collaboration between Industry and government:** The technology industry needs to collaborate closely with all levels of government, and clearly communicate the value proposition of blockchain technology and its potential role in the future economy – to address current hype about blockchain technology that can result in misinformation for lawmakers, regulators, lawmakers, and citizens alike. Furthermore, industry needs to demonstrate real production examples of blockchain technology deployment across various segments of the economy, such as supply chain management.
- **Increased research and test-bed deployments:** More resources need to be allocated toward this nascent yet rapidly evolving technology, much in the way the U.S. Government funded early research into the Internet in the 1970s and 1980s. It was this support from government, combined with a shared vision for a U.S. leadership role in initial Internet communications technology, that allowed the Internet to flourish with broad adoption and become the foundation of the digital economy today.

In sum, the roundtables demonstrated that addressing these common areas of leadership and vision from government, collaboration with industry, and support for research on future applications can help drive progress in enabling blockchain technology to support digital identity, payments, and supply chain innovations. The following appendices provide detail on these topics from the roundtables.

3. http://www.businessofgovernment.org/blog/how-can-blockchain-technology-help-government-drive-economic-activity-1

Appendix A

Roundtable Discussion: Unleashing Commerce with Blockchain Technology

A Blueprint Discussion on Identity

June 19, 2017
Washington, DC

INTRODUCTIONS

Thomas Hardjono, MIT Connection Science—Moderator

Summary

The meeting kicked-off with an introduction by the chair/moderator, Thomas Hardjono of MIT Connection Science, who provided high-level slides on the challenges around identity, blockchain, and data.

The purpose of the roundtable is to discuss the use of emerging technology, identify areas of common interest that can help accelerate adoption, and identify existing gaps that impede implementation. The specific goals for the "Identity & Blockchain" session is to identify components that are being uniformly examined across industries, businesses, and government agencies as important to maintaining integrity in blockchain technology.

The combined areas of identity and blockchain technology offer capabilities that were previously difficult to achieve, namely trust, transparency, and accountability. This combination poses a number of interesting challenges because identity covers enterprise identity management and consumer identity management. Blockchain technology also covers two broad areas, namely permissioned and permissionless blockchains. Add to this mix is the third axis, which is data that is the foundation of many applications is differing verticals. As such, the issues of privacy and confidentiality come to the forefront, enunciated by the specific needs of regulatory compliance, from Know Your Customers (KYC) to Anti-money Laundering (AML).

There is attractive synergy between identity and blockchain technology. Blockchain systems require membership management, which must be founded on strong and authentic identity. Conversely, blockchain technology may provide support for identity services to scale-up. What data is being recorded on the blockchain or linked from it becomes a third area of synergy, allowing data access, sharing, and user-consent to be auditable via the blockchain.

Discussion Points (Q&A)

- Rhetorical questions posed to attendees about what the difference is around the concepts of "trust" and "transparency" and then how that impacts "trustless" systems. Blockchain systems are often incorrectly referred to as "trustless."
- With respect to Identity and blockchain technology, there is a critical need to identify how identity services can "scale up" with the help of blockchain technologies and peer-to-peer (P2P) networks.
- Data around identity has become one the most valuable assets for an organization. Take banking for example. Many banks are envisioning that in the next decade they may not be in the "money business" solely, but also in the "trust" business because they have data of strong provenance and quality regarding people and customers.
- Attendees complimented this effort to create some foundational taxonomy but also challenged attendees to think about how we can "go to the next level"—emphasizing the need to adopt standards and to encourage leaders to "take the plunge" into blockchain.

NIST PRESENTATION

NIST, Cryptographic Technology Group, Computer Security Division

Summary

The mission of the National Institute of Standards and Technology (NIST) is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. Within the broader mission of NIST, the goal of the Computer Security Division is to conduct research, development, and outreach necessary to provide standards and guidelines, mechanisms, tools, metrics, and practices to protect information and information systems. A crucial part of this goal is to promote the adoption of strong cryptography through fundamental research, and the development of standards, guidelines, tools, and metrics.

As such, given the fundamental role of cryptography within blockchain technology, there is little doubt that NIST plays a crucial role in conducting and promoting research into relevant areas of blockchain technology—security, privacy, scalability, quantum resistance, etc.—as well as providing leadership in standardization efforts around this technology.

Examples of standardization efforts include the development of a common set of terminology and taxonomy, identification of relevant use cases, development of technical standards to ensure blockchain interoperability, and the identification of common primitives and building blocks underlying blockchain technology.

NIST has been very successful in identifying cryptographic primitives, and addressing the security quality of those primitives needed for U.S. industry and government needs. Examples include cryptographic hash functions (e.g., SHA family of hash function) and digital signature algorithms (e.g., EC-DSA family of algorithms).

Building on this expertise NIST is poised to address future crypto-schemes and algorithms that are relevant to blockchain technology. Some examples include ring signatures, threshold signatures, bit commitment schemes, zero knowledge proof techniques, multiparty computation, and quantum-resistant algorithms.

The topic of quantum-resistant algorithms cuts across all sectors and deployments of cryptography, including blockchain technologies and system based on them. This is because advances in quantum computing may render current or near-future algorithms to be "breakable" using quantum computing techniques, thereby affecting the immutability capabilities of blockchain technologies.

Current NIST activities in the area of blockchain technology include the establishment of an internal test bed to explore blockchain technologies and use cases. NIST has selected Hyperledger Fabric as one of three foundational blockchain technologies that they will include in their test bed, which is focused on testing and documenting Blockchain capabilities with an eye toward recommending standards and best practices for blockchain usage. The other two blockchain systems for the test bed will be MultiChain (Bitcoin API) and Ethereum (Mainnet). Currently, there is no timeline commitment to the completion of the test bed, due to limited resources within NIST.

In addition to current standards participation and investigations into use cases of blockchain technology, NIST is conducting foundational research in blockchain architectures, taxonomies, and cryptographic primitives. As part of its outreach efforts, in 2016 NIST conducted a "Blockchain and Healthcare Workshop" in collaboration of the Department of Health and Human Services (HHS).

Discussion Points (Q&A)

- Historically a core activity that NIST is working on is cryptographic algorithm standards.
- The presenter believes that more use cases need to be identified in order to control the current degree of "hype" and direct awareness into something useful.
- Largest areas that need more research:
    - Security of blockchain—Primitives, how they are being applied in blockchain? Underlying primitive needs to be used in secure way.
    - Privacy—It could be less private with permissionless than traditional technology, so add privacy but keep it scalable.
    - Scalability—Dominating question for permissionless blockchain, What is best way?
    - Consensus algorithms—How can you tweak to maximize properties you want?
    - Quantum-resistance—Potential for quantum computers to measure and attach block-chain crypto—hash and digital signature. There's a major effort at NIST around public key infrastructure (PKI) future; blockchain will be one of them.
- Additional efforts need to address standardization of blockchain related components, but NIST has limited bandwidth.
- Industry convergence on standardized terminology: Currently there are several efforts within different standards organizations and industry consortiums on terminology—ISO, IEEE, ANS X9, Hyperledger, W3C. These need to converge.
- A good analogy is from around five years ago where there was confusion in the cloud industry regarding terminology. NIST provided leadership by publishing guide document 800-145 covering terminology for cloud computing technology. So today we need an equivalent for blockchain terminology and taxonomy, use cases, blockchain interoperability, primitives, and building blocks.
- Cryptographic primitives: More and more proposals and architectures include new crypto-graphic primitives, including ring signatures, threshold signatures, bit-commitment schemes, zero knowledge proof techniques, multi-party computation, quantum resistant algorithms. There are large gaps in these area and standards are lacking. NIST has already been focusing on these research topics for a long time in, but only now hearing interest from industry based on certain use cases.
- Test bed within NIST: Currently NIST is setting up an internal test bed for three blockchain systems—Hyperledger, Ethereum, and Multichain. An attendee mentioned that a good approach would be to use the test bed to evaluate the various proposals on identity/ blockchain, in order to arrive at the best one for standardization.
- On-chain and off-chain functions: An attendee commented that blockchain systems may not ever be scalable to the levels needed—Visa and MasterCard process millions of transactions per second—and that the most heavy transactions will reside "off-chain"—or light on-chain, heavy off-chain. Examples of on-chain are anchor identifiers and qualified names; everything else is off-chain.
- Healthcare use cases: An attendee from a state Congressional office asked the NIST team for more details on health-related use cases that are being addressed by Health and Human Services (HHS) in the area of healthcare. She requested more information on the recent Nashville blockchain event, where winners used the Tierion solution.

- Provocative question: Do individuals really need or want to manage and control their health data? An attendee believes individuals may be overloaded if they had to manage all their data. The question was restated as individuals who need to be empowered to access heath data.
- Interoperability of standards: NIST team brought up standards and concerns over interoperability, especially with regards to cryptography standards. Several attendees commented that they would like to avoid getting too far too soon on technologies that end up not being widely used. An attendee added that government has a role to demonstrate "trustworthiness" of standards, avoiding the impression of "backdooring."
- Quantum computing: NIST team mentioned they are currently working with quantum computers to study upcoming capabilities that have the potential to affect blockchain technology and adoption.
- NIST guidance: A representative from Congressman Schweikert's office shared an anecdote on a narrow Veteran Administration's scheduling solution that was pitched to him last week after the Nashville hackathon. His general request to NIST is guidance with regards to specifications and standards, which will be used as the basis for procurement.
- Taxonomy guide or whitepaper: Several attendees mentioned that a NIST guide or taxonomy document would be useful to reduce confusion. A NIST attendee mentioned that such a document may be published in the future, but there is no commitment from NIST largely because blockchain is a new area. An attendee mentioned that the Kantara Trust Framework document has over 100 definitions.
- Best way to interface with NIST on this topic: NIST suggested the three NIST persons here today are the best and easiest contact points.
- NIST/HHS coordination: An attendee from a state Congressional office asked about how NIST and HHS coordinated for the 2016 HHS blockchain challenge. NIST was approached by HHS to review the 10-15 papers and submissions received by the HHS for that event. The general trend right now is to address the challenge of patient's control over health records that are exchanged through back channels. The MIT moderator mentioned that there is public concern about "who is doing what with my data" and that data access could be recorded on the blockchain. The risk could be that you mistakenly share information that is private or confidential.
- User control: An attendee mentioned that controlling access could be through data encryption. The more relevant question is how to give back useful and relevant information to the user. The attendee believes that Microsoft/Hyperledger/R3 do not compete on this point, and that NIST could evaluate whether the solution works the way it should.
- Standard cryptographic algorithms in current blockchains: An attendee mentioned that Bitcoin and Ethereum use different cryptographic algorithms. Ethereum uses KECCAK-256 instead of the usual SHA3 standard recommended by NIST. Can or should NIST provide recommendations specifically for blockchain systems? Aside from crypto algorithms, the area of privacy is one hindrance to broader adoption of blockchains. Bitcoin and Ethereum do not provide privacy. Can or should NIST provide recommendations? An attendee asked what if some blockchain systems use untested or not recommended algorithms? Should NIST look into these issues? It is difficult for NIST to do anything about this matter if implementers are going in different directions.
- Proposed Blockchain Naming Service: An attendee mentioned that there is a parallel between the classic Domain Name Service (DNS) underlying the Internet today, and the so-called "Blockchain Naming Service" (BNS), which is a proposal that provides name-to-blockchain resolution service. Such a service can resolve to identity hubs (collection of

personal data), as well as attestations and claims. The presenter from Microsoft states such a BNS service is months if not years away.

- Quantum computing: An attendee asked about the impact of quantum computing—quantum attacks—on blockchain transactions, notably the archive of blockchain historical transactions. NIST agreed about the concern that new quantum attacks can result in retroactive unauthorized changes to previous transactions.
- Longer cryptographic keys: In jest, an attendee mentioned that we should use one-terabyte keys. An attendee asked if NIST focused on cryptographic primitives. NIST responded in the affirmative but added that NIST depends to a degree on the work coming out of standards groups and industry consortiums. NIST asked, in turn, for input as to where NIST should focus its limited resources, and inqured about which industry groups and consortiums that NIST needs to collaborate with.

HYPERLEDGER PROJECT—LINUX FOUNDATION SESSION

Presented by IBM

Summary

The Hyperledger Project and development community is a technical and open source software development community focusing on a collaborative effort to advance cross-industry blockchain technologies. It is hosted within the Linux Foundation, which has been the premier open source software development community for the past two decades. All software is published under Apache License or MIT License, the two best license modes in the history of open source.

Within a short timeframe, Hyperledger has been very successful in attracting collaborators across a diverse sector, ranging from finance/banking to Internet of Things, supply chain management, manufacturing, and technology development. Hyperledger has proved to be the fastest growing project within the history of the Linux Foundation. This owes not only to the open source nature of the project, but also to the modular architecture of the Hyperledger design itself—allowing different modular components to be developed in parallel by different groups of developers.

Hyperledger uses the term “Framework” to denote meaningfully differentiated approaches to business blockchain frameworks developed by adjacent subgroups within Hyperledger. Examples include Fabric that focuses on the software stack that may be used by nodes within a blockchain system, Sawtooth that focuses on secure hardware-assist and other secure algorithms for Hyperledger nodes, and Indy for identity management.

The term “modules” is used to denote narrow components that are developed for specific Hyperledger framework, but which can be exported/shared to other related Hyperledger frameworks. Examples include the Composer, which allows business owners and developers to create smart contracts and blockchain applications; and the Explorer, which allows one to view, invoke, deploy, or query blocks, transactions, and their associated data.

Related to the focus of this Congressional Blockchain Caucus is the topic of identity and blockchain. Identity related functionalities are provided through the set of components within Hyperledger Fabric dealing with Membership. Among others, it includes a specialized digital certificate authority for issuing certificates to members of the blockchain network, and leverages the cryptographic functions provided by Hyperledger Fabric. Other components within Fabric are Consensus service, which enables digitally signed transactions to be proposed and validated by network members; and ChainCode, which expresses the transactions logic supported by the given instance of the Fabric deployment.

To date, the Hyperledger Fabric represents an industry-wide collaboration of 68 developers, representing 11 companies affecting about 80,000 lines of code.

As part of the industry deployment roadmap for Hyperledger, a number of reference deployments are underway across different sectors and verticals of industry—over a dozen. Examples include Everledger in the diamond trade industry for tracking the provenance of diamonds, the Depository Trust & Clearing Corporation (DTCC) in finance for the exchange of credit default swaps, and SecureKey for identity verification. IBM itself deploys Hyperledger within IBM Global Finance group—roughly 40,000 suppliers worldwide and 25,000 disputes annually—since September 2016 to reduce dispute resolution time. A Hyperledger blockchain is used to provide visibility and provenance end-to-end across supply chain, allowing the tracking of transaction information and evidence (e.g., contracts) within a given financing customer case.

The SecureKey/IBM effort is especially relevant for the current Congressional Blockchain Caucus on blockchain and identity. This joint effort is significant due to its successful pilot in Canada. A core part of the solution is that of "identity verification" in which strong sources of identity, such as government issued passports and bank information, is used in combination with a Hyperledger Fabric blockchain to provide membership management within the blockchain. In effect, the solution based on Fabric establishes an exchange that links digital asset providers—banks, telcos, government—with digital asset consumers such as merchants, businesses, and other relying parties. This exchange or bridge obviates the need for each relying party to repeat the cumbersome process of identity verification for an individual. Once an individual has been identity-verified by the SecureKey and Fabric system, multiple relying parties—primarily merchants—can query it and obtain the same strong assertion or claims regarding the individual.

The use of the Fabric blockchain means that no user data is visible to the intermediaries (e.g., network operator) and the distributed nature of the nodes on the Fabric blockchain means there is no centralized database that is susceptible to attacks and to failures. The SecureKey/Fabric system uses a triple-blind mechanism that prevents individuals from being tracked across relying parties with whom the individual transacts, thereby increasing the privacy of the end user on the blockchain.

Discussion Points (Q&A)

- Three areas of discussion: Major industry focus areas are (i) identity, (ii) payments, and (iii) provenance. An attendee mentioned that the topic "transaction" is back in-vogue again today, when he had spent the early part of his career at IBM on transaction systems.
- Identity in Hyperledger: In response to a question about the Membership function, the Hyperledger Fabric already has membership management—to use the moderator's phrase in the opening—as part of the permissioned model. This is notably useful for enterprises that want to deploy Hyperledger.
- Background history on Hyperledger: IBM has been a strong proponent of open source software for the past few decades, as evident from various open source projects listed in the Linux Foundation and elsewhere. Hyperledger itself originated from the need to have a blockchain software stack that was available under Apache License or MIT License. These license modes offer unrestricted access to and usage of the code, and therefore offer the best adoption course for the industry. (Note: Ethereum source code is available only under General Public License (GPL), which places restrictions on further development and usage.) Another factor in the decision to go the Hyperledger route is the need for the code

to be modular, with clear functional boundaries and application programming interfaces (APIs). Finally, the third reason for embarking on Hyperledger within the Linux Foundation is the excellent organizational governance that exists in the Linux Foundation. Thus, Hyperledger did not need to create its own governance model. It is for these reasons that IBM collaborated with Intel to begin establishing the Hyperledger Project.

- High quality of code: Hyperledger has one of the most rigorous "graduation" processes for open source code. New proposals for specific projects under Hyperledger must undergo an "incubation" period in which progress of the project is closely monitored by the Hyperledger Technical Committee, consisting of eight supervising organizations. The test coverage expected from a project is 85 percent or higher coverage. Prior to each update release, the code is scanned for security defects and weaknesses, in addition to the usual bug scans. High quality open source code is key to building applications on top of Hyperledger.
- SecureKey question: An attendee requested further information about the SecureKey and IBM joint effort in Canada. The presenter responded that SecureKey is one of 12 selected reference "customers" with whom IBM is collaborating to advance Hyperledger in industry. SecureKey is unique in the identity space because the SecureKey organization is the only one in Canada selected by the Canadian government a couple of years ago to conduct a pilot with the banking sector there. SecureKey has set up a digital exchange for identity-related information originating from Banks, which are guardians of accurate personal information and represent one of the pillars of society in Canada. The SecureKey model allows a person who wants to open a new account at Bank-X to ask the bank to "Verify Me" (analogous to "Friend Me") through the SecureKey exchange. The exchange will return information with strong provenance about the person, thereby obviating the need for Bank-X to request paperwork for the person. This streamline process reduces cost and friction immensely. The "Verify Me" process is controlled by the individual whose data pertains to the process. There is no "honey-pot" or "social media" involved.
- Future plans question: Question from audience regarding a U.S. version. The SecureKey/IBM pilot involves all seven major banks in Canada. As such it represents a pilot with well-defined boundaries and scaling properties. IBM and SecureKey are currently working towards bringing a similar pilot to the U.S.

HYPERLEDGER INDY– LINUX FOUNDATION SESSION

Presented by Project Indy & Sovrin Foundation

Summary

The Hyperledger Indy Project focuses on identity management using the frameworks and components of Hyperledger. The project originated as code that was contributed by the Sovrin Foundation, and has as its goal the creation of the portability, scalability, and privacy of self-sovereign identity.

A feature of Indy is the use of Decentralized Identifiers (DIDs). DIDs allow for a decentralized architecture to be deployed and perform resolution-mapping from a DID-identifier to information about the user located on a blockchain. The mapping is cryptographically verifiable, allowing a relying party in a transaction to obtain assurance that the information the blockchain is authentic without relying on the Domain Name System (DNS) infrastructure. A key concept here is that DID is permanent and portable for the lifetime of the user who is associ-

ated with the DID. Previously, the DID concept was developed under a grant from DHS Science and Technology. As next steps, the Indy projects is seeking to make the DID a standard through the World Wide Web Consortium (W3C). The DID is independent from the specific type of distributed ledger, both permissioned or permissionless.

The overall goal for the Sovrin Foundation is to address the broad set of use cases involving permissioned public distributed ledgers, where Sovrin becomes a global public utility for self-sovereign identity. The Sovrin ecosystem involves three layers of entities, with the core consisting of a pool of Sovrin Validators whose task is to validate the ledger on an on-going basis. These entities are grouped into the Ledger Validator Pool. A second layer of entities is denoted as the Ledger Observer Pool, while the third layer is Cloud Agents and Wallets.

The purpose of the Sovrin three-layer architecture is to allow the exchange of secure private verifiable claims via the P2P network that is layered on top of the Sovrin ledger. Parties or users who are transacting are assumed to be using Edge Agents or Wallets that facilitate the ease of obtaining verifiable claims, providing increased assurance by one party to the other, and vice versa. The verifiable claim is a digitally signed assertion that represents an alternative to paper-based official records reduces/mitigates forgery and counterfeiting.

The first mass market use of the Sovrin architecture is by CULedger, which is a cooperative distributed ledger project of the U.S. credit union industry. The first application for CULedger is the reduction of call-center fraud for credit union members. When a credit union member or user calls a union call center, the call center system looks of the DID of the user on the Sovrin ledger. Similarly, the app on the user device looks up the DID of the call center on the Sovrin ledger. An identity agent—part of the Sovrin Cloud Agent layer—mediates an authentication event between the user device and the call center system, with the user device returning a cryptographically-signed approval to the call center system.

Discussion Points (Q&A)

- Scope of Sovrin identity: Responding to a question from the audience, the presenter mentioned that the goal of Sovrin is to address "self-sovereign" identity at a global scale, beyond the permissioned model. The Sovrin Foundation has already donated code into the Indy project, and plans to continue development of the code.
- CULedger and proof of identity: The audience member form CULedger relates the anecdote of him receiving a phone call from a credit union. The caller was asking personal information over the phone as a method of authentication. However, it became clear that "mutual proof of identity" was needed so that both sides could obtain assurance about the identity of the other person.
- Grants to accelerate adoption: Indy within Hyperledger is the first use of DIDs as "privacy respecting identity management" under a DHS grant. So yes, grants from the government or other institutions may accelerate work in Indy and its adoption in the market.

DECENTRALIZED IDENTITY FOUNDATION

Presented by Microsoft Identity Division

Summary

The Decentralized Identity Foundation (DIF) is a Microsoft-led effort to create a blockchain-anchored identity ecosystem. The three-point thesis of the DIF proposal is (i) the use of the

blockchain is the anchor, (ii) decentralized identity is the platform, and (iii) perfect information is the app and service revolution.

The DIF model relies on off-chain identifiers and timestamps. A blockchain transaction is embedded with ID registration data. This transaction contains proof of who the ID-owner is, and where their data resides (off-chain). All off-chain identity data is signed with the private key of the ID-owner to prove its authenticity.

The DIF architecture has three layers, consisting of the blockchain system, an ID registration and index system, and a mesh of identity hubs. An identity hub is a set of identity data that is replicated on multiple storage units on the cloud and at client hub instances. End-to-end encryption is used with a "Trust No One" default state for external instances. Data access to a hub is determined by the user. All hubs, regardless of implementation or provider, use the same self-describing API based on standard schemas already widely used across industries.

For the end user, identity attestations enable the user to own valuable proofs about the user, and expose them to whomever the user chooses. Using the example of LinkedIn, the attestation layer creates new opportunities for apps. As an example, a prospective employer of a user may check the education qualifications of the user on LinkedIn, where the LinkedIn system generates and validates attestations.

For organizational identity management, the Microsoft Azure Active Directory (AAD) attestation management feature will allow organizations to create, manage, and enforce the same facets of identity via "Bring Your Own Identity" model.

Discussion Points (Q&A)

- Rights to data: In response to a question regarding the "ownership" of data, the presenter states a libertarian view that citizens have rights to their own data.
- LinkedIn model for attestations: In the case of the LinkedIn data example, the user (Jane, who has a degree from University X) is not concerned about the information being visible to the public. Instead the concern is about the authenticity of the claim, which is relevant for recruiters and other relying parties. So, the university should sign these claims. The value is really in owning the process of registrars verifying the information in a claim.
- Enterprise scenario: The presenter mentioned Azure Active Directory (AAD) as the basis for enterprise identity management, which recognizes personal identity and business identity.

OPEN DISCUSSION SESSION

The open discussion session addressed the topics of (a) proof of identity, (b) security and trustworthiness, and (c) interoperability and ease of use.

(a) Proof of identity

- Onboarding model: The representative from the credit union stated that everything in their process relies on correct identification and identity. The moderator asked is the old paper-based onboarding model could be used as the basis for onboarding into a blockchain-based solution. The answer is, "Yes, it is inevitable."

- Ownership of identity: Regarding ownership of an identity, questions were asked—Is it the Social Security Administration's or is it more of the "right to use" an identity? Does my data reside under my control? For example, if I reveal my Social Security numbers (SSN) to you, do I remain the sole person who can assert it as proof of identity? A number of start-ups—Tierion, Civic, Blockstack, etc.—are facing the problem of compliance to Know Your Customer (KYC) regulations.
- Governance model over attestations: In an audience comment regarding the need for a governance model and standards over attestations or claims, the response from another person was that this is a separate question from blockchains. Related to this is the current method used by the U.S. government to deliver SSNs—23 million postal mailings annually. Here the government plays a key role in ensuring interoperability of entities in the ecosystem, even though this SSN dissemination mechanism is still in the paper world.

(b) Security and trustworthiness

The next topic was the security and trustworthiness of identity systems tied to blockchains. The moderator specifically asked two hardware/chipset companies present to address this topic.

- Security vs. privacy vs. efficiency: There is the question of error in identity systems, even in systems deemed to be secure. As such, how is this different from today's more manual method using a human verifier? We could architect the system to be better—less errors—to begin with. Let's reimagine the web, start with document-based identity and move to digital identity. One audience member cites the Microsoft Smart Cities waste management as an example.
- Business design patterns: Are we getting security/crypto right for this new world of identity and blockchains? Trusted hardware exists today that can be leveraged.
- Minimal questions to ask the user: Verifiers and relying parties should ask just enough questions to get the task done. This is what NIST 800-63 prescribes. We also need to focus and spend money on better user experience to reduce errors and to obtain user buy-in.
- Readiness to deploy: In a question about readiness, an attendee noted that this depends on the components of blockchain-based identity. Some parts, such as name-to-blockchain resolution systems analogous to DNS, will be ready in a matter of months. But other components, such as user consent management, data privacy, and increased performance of the blockchain transaction processing, may still need time to evolve.
- Disintermediation: In a comment from the audience that the promise of blockchain is one of disintermediation from a centralized authority, an attendee response was that some governments are already working towards "self-sovereign identities." He cited the Austrian case and use of the "Web of Trust" paradigm. A follow-up question: Can government be the central identity authenticator in the "Web of Trust"? The answer depends of the specific case or the specific ecosystem.
- Key and credential management: A hardware manufacturer commented that cryptographic keys and credentials are difficult to manage by the end-user, and that many consumers do not know how to protect their keys. In many vases, an attack is successful because the password is compromised through social means—not because the hardware is compromised. There are currently products out there—from Qualcomm/Intel/IBM, for example—for enterprise security that uses special trusted hardware so that keys and credential are very difficult or expensive to steal. However, many of these enterprise solutions are inap-

propriate to use for the consumer space. And today there is no guidance either for "digital exchanges" (e.g., digital currency exchange systems). Another attendee commented that the data in user mobile devices should be considered as protected under the Fourth Amendment where the government cannot search it without a warrant.

(c) Interoperability and ease of use

- Leadership in digital commerce: An audience member stated that there is a leadership role for government in the future area of digital commerce, based on blockchain technology, through policies and regulations. There is also the question of how to "enable" these leaders with business models that derive value. Another person cites the Estonia case where the government has been active in the space of identity and blockchains. Another audience member cites the minister in Great Britain who provides "leadership from above."
- A layered model: An attendee from the payments industry suggested that we should look at a layered model, where data and the audit trace are separated—Layer 1. Within Layer 2, use a peer-to-peer model to alleviate scalability issues. He cites the current card-payment network that can process over 10,000 transactions per second. Then Layer 3 is where the business logic and rules are expressed, as smart contracts, and where the state-transitions for transactions are defined. There is a need today for a "shared language" to discuss or describe the core aspects of the blockchain-based system. The shared language must include clarity on concepts such as permissioned, non-permissioned, private, public blockchains. This is complicated technology, involving complex crypto (not just hash functions), crypto-schemes, and algorithms.
- Leadership by the U.S. government: An audience member states that we have already identified a number of great use cases for blockchain technology. We need someone to "have their backs" to encourage going out and being a leader in this space. We need to have guidelines/best practices, not legislation or onerous rules, around different ways government will interact with blockchain networks. Some possible roles for the government:
  - Participating in blockchain networks, likely as regulators
  - Bringing together and sponsoring a business network to solve a tactical problem and drive value (smaller, easier, quick win) across the business network on top of the existing process
  - Bringing together and sponsoring a business network to address a long-term challenge or consider digital reinvention

Appendix B

Roundtable Discussion: Unleashing Commerce with Blockchain Technology

A Blueprint Discussion on Payments

February 21, 2018
Phoenix, AZ

INTRODUCTIONS

Thomas Hardjono, MIT Connection Science—Moderator

OPENING PRESENTATION: Congressman Schweikert

Congressman Schweikert provided an engaging opening by posing a number of use cases, scenarios and possibilities for blockchain technology. These use cases range from smart contract code related to autonomous vehicles (e.g., code correctness, risk assessment, liabilities, etc.), title ownership (e.g., land title), state-based transactions on a micro scale (e.g., micro-savings for citizens' 401K), identity management and verification, medical wearables, and so on.

Discussion Points (Q&A)

- An audience member raised the question of viewing the trust aspect of the blockchain improperly or in an incomplete fashion. Initially legislative acceptance might need to be "forced," with the cascading effect of actual improvements, then allowing for more seamless regulatory transition. Right now, government is not set up to have transparency and enforcement within the same system, where the legal standing via public record and identities can be verified and transacted in a single system.
- Another question from the audience touched on blockchain technology as a multidisciplinary problem, and how to create an environment in which all of these different disciplines can work together—public, private, academic, corporate, etc. Aside from the need to continually improve the technological aspects of blockchains, such as better consensus mechanisms, there also needs to be efforts to close the gap between experts in other domains, such as economics and healthcare, and with non-technical community members. New forms of "sandboxes" for experimentation are needed to allow these kinds of partnerships to flourish.

PRESENTATION: JOUST BANK

Summary

The presentation from Joust Bank addressed the various aspects of digitizing privacy with regards to banks' requirements for privacy, and KYC rules. The presentation started with a review of the history of Joust, which originated from the presenter's previous start-up, called Tokken.

The main purpose of Tokken was to provide payment services to an underserviced or unserviced sector of the local economy in Colorado, namely the cannabis retail sector. In developing Tokken payments services, a crucial issue needed to be solved, namely verifying the identity of the payer and user as part of the KYC/AML process. As part of the on-boarding process for enabling payment services for new users, Tokken developed proprietary mechanisms based on back-end data to verify the user's historical background.

Each transaction then involved performing algorithmic analysis on each user based on their name, phone number, etc. Similarly, for KYC/AML requirements each merchant's background is assessed and an algorithmically generated "trust score" is assigned to the merchant. In the area of blockchains, Tokken employed a blockchain system to store a hash of the merchant/user metadata in order to provide data integrity and tamper detection.

Currently, Joust is expanding to address the grown "gig economy," which is projected to be a $2.2 trillion economy. One key problem in the emerging gig economy is that freelancers, who cannot always collect on non-payments, are ostracized from protections afforded to traditional corporations. On the client side, there is the question about the identity and authenticity of claims put forward by freelancers. To address these issues, Joust has created services to provide instant payments to freelancers, insurance of invoices, credit access, and interoperability with tools traditionally provided by corporations, such as health benefits.

For example, for invoice insurance, Joust provides up to 75 percent of coverage and uses a rewards system based in cryptography and a risk dispersal system for each transaction. Freelancers build "crypto-rewards" within this system that can be spent outside the system. These "crypto-rewards" can be viewed as either a "currency token" or as a "security token" depending on how it is deployed.

As next steps, Joust is developing a mechanism to "monetize the future work potential" of any given freelancer. As part of this, Joust is developing a trusted platform for the gig economy on which to transact—one that ensures traditional risk mitigations and rewards.

PRESENTATION: RIPPLE

Summary

The presentation from Ripple provides an overview of the Ripple payment system and the future directions of the payment service based on blockchain technology. One key aspect is the removal—disintermediation—of a central party from the payment process, allowing financial institutions to connect to each other in a global fashion. Companies use the Ripple service agreement upon the fee and FX structure beforehand, and as such, prevent delays in transmissions. Looking to the future, Ripple plans to pursue high-volume, low-value payments and notably focus on the area of remittances for small businesses seeking growth.

The existing KYC/AML processes remain unchanged for current processes. The KYC/AML must be performed by the financial institution, and Ripple provides the software—xCurrent—that plugs into the institution's existing solutions. As such, a bank that seeks to use Ripple needs to determine which other banks they want to do business with and address the requirements of U.S. regulations and other relevant regulations. Using the Ripple software, the bank can choose to connect to xCurrent or the XRP exchange. Both of these rely on a private blockchain that is owned and operated by Ripple.

The Ripple xCurrent ledger software sits between transacting financial institutions and provides a messaging service and settlement infrastructure. The blockchain speed is fast due to Ripple's proprietary two-step consensus protocol. The xCurrent software simplifies inter-bank transactions because the banks are essentially agreeing to the blockchain-governance terms provided by Ripple when they access this ledger software. The task of performing due diligence must be conducted by the banks seeking to transact and is performed outside xCurrent. Thus, Ripple serves as an additional rail for the transactions to flow but the normal regulatory obligations of the banks still fall to them.

The XRP unit acts as a liquidity tool by complimenting fiat currency. Banks agree to FX rate for XRP beforehand, allowing for quick liquidity without costly intermediary rates. It is important to note that there is no XRP exposure to consumers.

With regards to the often-asked question of XRP being digital assets or virtual currency, the XRP is used solely for fiat exchange and therefore it does not hold the value during the transfer of XRP through the Ripple network. Thus, XRP is transactional only. However, this does not preclude banks from holding XRPs for future transactions.

OPEN DISCUSSION SESSION: DIGITAL CURRENCY

- What is the nature of a currency: Money exists as a consequence of our society. Currency is a tool for something, not a thing in and of itself. It must be durable, portable, divisible. It's a way to facilitate certain transactions. It's been said money is memory, where transactions are based on the value of what you have done for people. It's not only as a tool to exchange goods and services.
- Social aspects of money/currency: There is a social perception about money. It needs to be perceived as "safe" to be used by people in society. The value of using a currency comes from the "insurance" (and assurance) that the government will not print an infinite amount of it, increasing inflation or insurance in a monetary form. As a discussion example, Venezuela recently declared it was going to issue its own digital currency, as a means to forego issues with their own paper/fiat currency and its volatility.
- Redistribution of money: When paper/fiat is exchanged for digital currency, it does not disappear. Inflation comes from having two assets with value. Relative value of assets change, but nothing else can change. For example, I can buy more milk with one vs. the other. In reality, today most money is electronic today. There is roughly $1 trillion in physical currency and roughly $18 trillion in economic value for U.S.
- Exploration of future digital currencies: Exploration is needed of use cases to drive adoption of new digital currencies. For example, cases where price of transactions approach near zero, and cases where money is flowing only through certain transaction types. Economics of certain markets lend themselves to digital currencies. These cases involve the removal some of the extra costs to using traditional streams that are normally passed onto the consumer.
- Government issued digital currency: If the government adopts blockchain for the issuance of currency, it remains fiat if they have control of the issuance and retention of money. There is also the issue of the resiliency of currency. In fiat currency, a government cannot print more to handle national debt or cannot tax its way out of it, or it will destroy its economy. Central bank could issue a digital currency/asset into the public domain accessible to consumers and businesses, but this means the bank cannot keep the currency within its own borders. The extended effect is that it could become the liquidity supplier for the whole world and when this happens it could be interesting how the world reacts. Central bank money requires them or a third party to get involved to perform KYC/AML, and we need new innovative ways to do KYC/AML.
- Governance and idea of consensus: There seems to be a misunderstanding about "consensus" and consensus-algorithms. The current proof-of-work paradigm—also known as Bitcoin—is not sustainable. There needs to be exploration into the balance needed between a "governed network" where access is controlled/granted versus an open network that is "self-governed." This is not just an engineering problem, but involves legal and regulation. For example, the U.S. judicial system doesn't need participation or "consensus" of the entire nation to convict a felon. So, in fact, we have a "delegated consensus."
- Policies today and into the future: There may be different considerations for digital currencies that represent different asset classes. Today fiat currency is based on "sentiment" and when a loss of sentiment occurs, problems and criticisms will arise. This results in the population losing belief in the currency, which can be catastrophic to a

nation. Interest would be high for a digital currency that is as stable and boring as the greenback. Many other benefits will also come with this inherently digital nature. The economic losers would be those that are too slow to adapt or adopt new policy for this kind of technological advancement. Gross domestic product (GDP) growth could come from taking friction out of these systems.

- Incentives to innovate in economy-technology sector: Comment from the audience that the rest of the world is adopting these digital currency policies and technology faster and more efficiently than the U.S., which is bringing them GDP growth. New incentive systems for businesses can stem from these advances. Currency officers of SEC-traded companies are beholden to the shareholders but think of a new model where the customer/consumers as direct owners or shareholders.
- Creating a sandbox for experimentation and innovation: What does this sandbox look like for experimenting with these technologies and ideas? A framework is needed for people in the U.S. to safely experiment with these blockchain networks and currency ideations. Currently regulators are overseeing this issue—five at the federal level, 50 at the state level. Individual states might be the best bet for this sandbox, since they can experiment without the federal government weighing in. Each state can create its own idea of the sandbox, even if it infringes on the federal government's prevue if the state is willing to take on the responsibilities. A key point is that the Financial Crimes Enforcement Network (FinCEN) must not issue no-action-letters for these types of jurisdictional issues—or else it will discourage innovation at the state level.
- Baseline for innovation sandboxes: Baseline is a key aspect—there needs to be baseline agreements for the types of experiments, structure, consumer protection, etc. This provides protection for the states. You can enforce consumer protection rules without needing to enforce regulatory rules in this sandbox. But we must have federal buy-in for these state-led initiatives. The Financial Stability Oversight Council (FSOC) could be a viable entry point for this. It has oversight into many different federal regulators. The sandbox should be inclusive of issues of digital identity, payments, and supply chain. Setting high bars for these sandboxes can prevent or discourage further innovation. There are legal issues in creating these sandboxes, such as lawsuits brought against them.
- New discipline of economic technology: It's a new term for this emerging discipline or field of study. Economic technology is crucial for the future of the U.S. economy. Government policy needs to catch up fast to DLT, blockchain, currencies, etc., because this is critical economic technology. A distinction needs to be made between the technology and their economic implications to the citizens. This type of technology can be so disruptive that it needs to be reviewed, studied, invested in—or else the U.S. could critically fall behind.

OPEN DISCUSSION SESSION: IDEATION FOR LETTER OF RECOMMENDATION

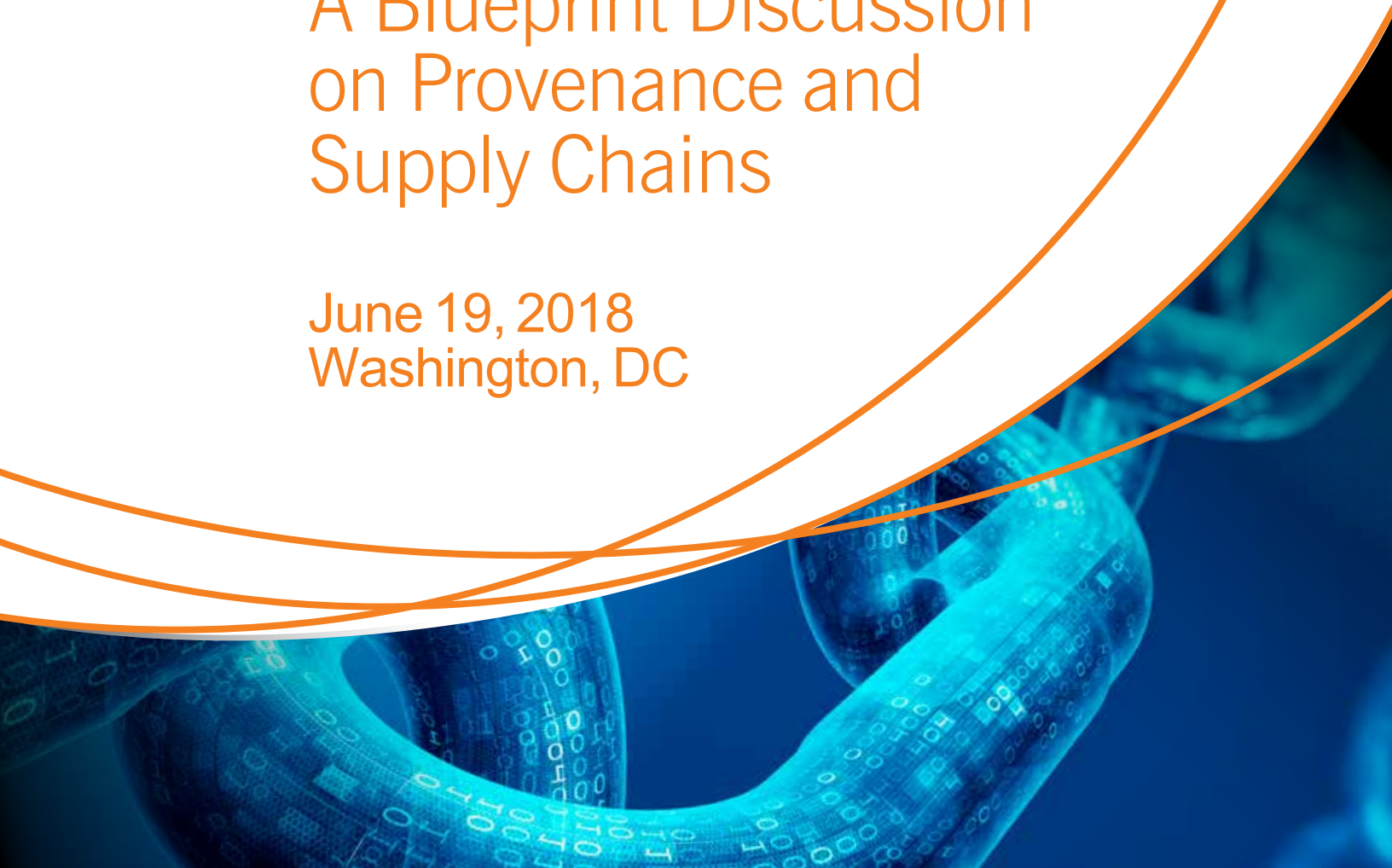
- Idea for letter of recommendation: An attendee suggested that the group consider writing a letter of recommendation to the relevant federal authorities, identifying issues and proposed solutions. The following is a list of possible items that could be addressed in the letter:
  - Agreement on the definition of digital currency: Provide a definition of the terms, such as digital currency, blockchains, virtual currency, among others.
  - Outline of the concept of sandbox: The notion that Congress could create a "safe space"—at the states level or at the federal level—for innovation to be tested, studied, and evaluated as a way to gain knowledge that can correctly inform regulation at a future date.
  - Hand-on approach on in sandboxes: Invite private sector entities as well as regulators to take a "hands-on" participation in these sandboxes, as a way to gain deeper understanding of the technologies, benefits, and challenges.
  - Closer engagement between regulators and innovators: The need for a close and ongoing dialogue between regulators and innovators, as the basis to obtain clarity in these fast-moving spaces. This is a multidisciplinary problem.
  - Request to Congress: Look into the possibly of asking Congress to pass a bill that provides U.S. states with the right to establish sandboxes for experimentation in collaboration with the various regulatory agencies, with the guarantee that states will not receive a no-action letter from these regulatory agencies.

Appendix C

Roundtable Discussion: Unleashing Commerce with Blockchain Technology

A Blueprint Discussion on Provenance and Supply Chains

June 19, 2018
Washington, DC



INTRODUCTIONS

Thomas Hardjono, MIT Connection Science—Moderator

Summary

The meeting kicked-off with an introduction by the moderator of the meeting, providing general rules of conduct and high-level slides on the challenges around identity, blockchain, and data.

The purpose of the roundtable is to discuss the use of emerging technology, identify areas of common interest that can help accelerate adoption, and identify existing gaps that impede implementation. The specific goals for the "Provenance, Supply Chains & Blockchain" session is to identify components that are being uniformly examined across industries, businesses, and government agencies as important to maintaining integrity in blockchain technology.

The three broad categories of provenance addressed in the roundtable are as follows:

- Supply chain for the provenance of contracts and agreements: How can blockchain technology improve the accuracy, efficiency, and transparency of the various contracts within the workflow of a given supply chain management ecosystem, such as contracts in the shipping and music industries.
- Supply chain for the provenance of logistics of goods: How can blockchain technology be used to track the movement of goods, in combination with Internet of Things data, and provide better transparency in the course of detecting and preventing the circulation of counterfeit goods, such as counterfeit medicine and high value goods.
- Supply chain for the provenance of data and information: With many organizations today overwhelmed with digital information and data—both sourced internally and from external sources—how can blockchain technology help organizations manage the workflow of data and the movement of data within the organization. Organizational decision-making relies on good quality data and information with known provenance.

NIST PRESENTATION—BLOCKCHAIN AND SUPPLY CHAINS

NIST Applied Cybersecurity Division

Summary

The mission of NIST is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

NIST has been focusing on blockchain technology for some years now. Activities include the development of "workbench" for blockchains that allows NIST researchers to experiment on different aspects of the technology. More recently, NIST published the NIST IR 8202 (draft, January 2018), providing a high-level technical overview of blockchain technology, including applications in the areas of supply chain management and automation. This report is expected to be finalized over the next few months.

Another activity is in the International Standards Organization (ISO), specifically ISO/TC 307 on Blockchain and distributed ledger technologies. The TC307 work groups cover several areas, including identity management, smart contracts, and interoperability. Interoperability is a key aspect of blockchain technology to ensure the realization of the true potential of the

technology. This effort represents a joint effort with the European Union. Researchers at NIST are also applying formal methods techniques on smart contracts, which is essentially code on blockchains for formal verification, malware detection, and so forth.

Specific to supply chain, the work at NIST—from IT technology to security—covers both (i) technology supply chain management, and (ii) technology for infrastructure for supply chain management. These seek to address various issues, including counterfeit components in IT; poor quality of manufacturing, maintenance and disposal; malware insertion into the hardware/software management lifecycle; vulnerabilities in the networks used by supply chain partners; and so on. The result of these efforts at NIST provides input into the NIST guidance for agencies, disseminated through the various NIST publications and consultations with these government agencies. Furthermore, these "lessons learned" become input into directives and standards, such as the Office of Management and Budget (OMB).

Discussion Points (Q&A)

- Interoperability of blockchains: NIST is studying this area because it is important for the success of the technology. A simple example would be how one blockchain could read or refer to the metadata in the blocks of transactions in a different blockchain. The moderator suggests that the Defense Advanced Research Projects Agency's (DARPA) principles for the development of the Internet in the 1970s could be used for interoperability of blockchains.
- Quantum computer vulnerability: If the fundamentals of cryptography breakdown in the face of quantum type attacks, what avenues are available? Currently, several NIST researchers are studying this area of quantum cryptography, including how blockchain technology can be impacted and how it can contribute to solving the problem. Examples are the NIST efforts to lead the Post-Quantum Cryptography Standardization process. NIST is also studying the possible use of blockchains as a source for random number generators. A person in the audience mentioned the recent government announcement to fund quantum "proofing" from NIST, National Science Foundation (NSF), and Department of Energy (DOE).

PRESENTATION ON PROVENENACE OF DATA: ENDOR

Summary

The presentation from Endor covered the use of blockchain technology as a means to manage the supply chain of data and information. The hash-chain of blocks, or transactions, represents at the micro level a "supply chain" of information pertaining to the records of transactions occurring on the blockchain itself. However, the work at Endor seeks to push the boundary further by taking into account (a) the off-chain data located at the nodes of the P2P nodes of the blockchain, where this data is possibly encrypted, and (b) using the blockchain itself as a means to connects users, or buyers of information with the suppliers/data owners of the encrypted data coupled with analytics capabilities (i.e. algorithms).

Endor is a start-up company out of MIT and now based in Israel. Endor is using blockchain to bring to the fore three major innovations that leverage the outstanding social physics-based prediction engine:

1. Crowdsourcing of expertise enabling anyone to contribute to the improvement of the algorithms and get rewarded in tokens, which they can further use to obtain predictions

2. Using a token to incentivize data providers to integrate additional data sources to the Endor Protocol, improving predictions' accuracy.

3. An unprecedented way to enable the merging of legacy infrastructure with novel blockchain services, thus supporting the transition of the big enterprise customers to the Endor protocol in order to have access to better predictions which use our larger pool of aggregate data.

The technological advancement offered by Endor is the ability to run aggregate analytics over encrypted data without any keys. The solution is able to provide answers while preserving the privacy of the data owners and of the data-subjects whose data may be in the encrypted data set. Furthermore, because data is always in an encrypted state, the owners may be more open to uploading copies to a cloud platform. Aside from developing the cloud-based platform, Endor is also focusing on using the P2P nodes of blockchains as a means of making a broader set of encrypted data available to a broader set of users. Thus, users and information seekers can "search" for relevant sets of data on the nodes of blockchains, issue predictive aggregate-type questions with payment, and obtain responses that are privacy-preserving. This approach provides greater compliance to the EU's General Data Protection Regulation, or GDPR.

In addition, Endor has released the Endor Protocol—an open source specification that allows developers of prediction engines to integrate with the sellers and buyers and generate these predictions. As long as these prediction engines comply with the Endor Protocol, they can use whatever technology they wish in order to improve accuracy and reduce computational requirement—all this while operating on the same data, and thus still maintaining data privacy and GDPR compliance.

While most large organizations are contemplating whether to implement blockchain for its value as a "Truth Machine," a shared immutable ledger—Endor is pioneering the use of a token to include large enterprises into the Endor Protocol blockchain ecosystem. This convergence of platforms will ensure a larger pool of aggregate data processed on the Endor Protocol, which will not only enable an increased volume of predictions on the Endor Protocol, but also is expected to continuously improve predictions quality.

Endor is the first ever to integrate both an enterprise business and a crypto protocol feeding into each other naturally to deliver best results for everyone through access to more data and a larger range of improved predictions.

The long-term goal of Endor is to create an ecosystem that makes analytics capabilities available to the ordinary person, and thus democratizing the power of AI—and thus become the "Google of predictive analytics questions." Part of this effort is developing the suitable incentives and remuneration model based on our unique token economics.

Discussion Points (Q&A)

- The right to be forgotten: Endor as a platform provides only aggregate level answers on predictive analytics over encrypted data. As such, it does not return answers questions that re-identify individuals. The question of the right-to-be forgotten lies in the owners of the data who encrypt the data prior to making it accessible to the Endor analytics engine.
- Support for Bancor protocol: In response to an audience member's question, Endor is collaborating with Bancor to explore various remuneration models for both the data owners and the users. This is part of Endor's efforts to become the standard protocol for predictions, to be used by various blockchain infrastructures. Bancor is one example, where Endor can increase efficiency of liquidity allocation. Another example is ORBS—a scalable blockchain for consumer applications where all the projects powered by ORBS will have built-in access to Endor predictions that are inherently GDPR compliant and privacy preserving. Endor is discussing similar partnership with leading blockchain infrastructures like Cardano, Enigma, HOLA, and others.
- Healthcare data sharing: An audience member asks about the possible use of Endor technology to help address the current crises in opioid addiction. The Endor model allows competing pharmaceutical companies to share insights, but not raw data because all data is encrypted prior to being run with the Endor analytics engine. As such, it could be used to help the government and the pharmaceutical industry obtain better insight into opioid trends and provide some predictive capabilities about this trend.
- Individual ownership of data: An audience member comments about the need for individuals to have ownership rights over their data, and for data on blockchains to be free from personally identifiable information (PII). The moderator agrees and points to the World Economic Forum (WEF) report from 2011 on personal data as the new assets class and its direct influence on General Data Protection Regulation (GDPR) regulations. The moderator also comments that in the U.S. perhaps the best approach is the "information fiduciary" approach put forward by Professor Balkin of Yale Law School. The Endor technology can be used to implement a method for providing individuals the possibility to define which queries can access data relevant to them and which cannot. This can be done either in an opt-in or opt-out manner, allowing individuals to control which service is granted access to their information. Please note that this is a further layer of privacy, on top of the data encryption, as individuals cannot only be guaranteed that they are not being identified, or that they have the right to be forgotten, but can also be compensated financially when their data is used—even if it being used as part of an encrypted, aggregated dataset.
- The ask from the government: The government allows for so-called sandboxes for exploration to be created, focusing on other uses of blockchain technology, such as for off-chain storage of encrypted data and token-based services. Endor is the leader of the MIT Crypto and Blockchain Systems Alliance, dedicated to promote and fund research in these topics, and would happily assist the creation of sandboxes. If required, such a sandbox can also be created at MIT, giving access to academic researchers, as well as the public. One crucial pain point that Endor can undertake is digital currency fraud, as underlined in the recent executive order on market integrity and consumer fraud, (https://www.whitehouse.gov/presidential-actions/executive-order-regarding-establishment-task-force-market-integrity-consumer-fraud/). Since the technology can detect patterns of fraudulent behavior and single out the culprits, Endor can support anti-money laundering efforts, both in the fiat and cryptocurrency space.

PRESENTATION ON SUPPLY CHAIN OF CONTRACTS: SWEETBRIDGE

Summary

The presentation from SweetBridge covered blockchain technology as the basis for managing digital contracts and digitized assets, including smart contracts as legally binding agreements. SweetBridge is developing a protocol that is open source, community-driven, and tech-agnostic—touted as the operating system for business. The world is currently entering the decentralization era, ushered in by the introduction of blockchain technology. The decentralization model applies not only to products and supply chain logistics, but also to capital management and risk management. The SweetBridge protocol sees the supply chain as consisting of several parts, namely legal, identity, accounting, and payments.

Currently the accuracy of information within supply chains is poor and low quality. The presenter cites some data points obtained from a study: an example of 200 million data points obtained from studying supply-chain data files from a transaction set of $2 billion in value. Almost 99 percent of the data—files within the supply chain management—contain one or more errors. Out of these, about 19 percent possess significant errors such that these files cannot be uploaded into enterprise resource planning (ERP) without considerable adjustments/corrections by human intervention. About seven percent contain financial information errors. This maps to 54 basis points, or about $160 trillion. One of the key issues is that the paperwork and the goods/items were moved through different channels in the supply chains. In many stages through the supply chain, paperwork was manually modified or appended, correctly or incorrectly, in order to push the goods through, leading to many inconsistencies in the final state.

The SweetBridge protocol seeks to create atomic transactions that synchronize across these four parts—legal, identity, accounting and payments. The protocol uses a kind of "voucher" construct to maintain information regarding the identities of people and assets, signed digitally by all relevant parties, and all the data synchronized. Using blockchain technology, the vouchers can cross-reference, or link, to one another across different systems. Additionally, SweetBridge is developing a "wallet" to hold these components, including agreements and assets, and also investigating the use of payment without money, or payment using assets.

SweetBridge sees the potential to unlock the trillions of dollars of value of sitting inventory—the average time of inventory sitting is 54 days. There is important correlation from the accounting perspective, namely that as the owner of assets, an entity is also the owner of liabilities. As such, these two aspects of business must never be out of sync, which it is today. The SweetBridge blockchain seeks to provide this tight sync.

Discussion Points (Q&A)

- Synchronization question: How do you synchronize all the data with a physical asset with time lag? The accounting system drives everything as activity gets written on the blockchain. The accounting system is independent of any blockchain but uses information captured on the blockchain.
- Comparison with Knight capital: How do you avoid the downfall of Knight capital? Algorithmic trading, resulted in a rogue algorithm, resulted in financial disaster for company. The SweetBridge arbitration board governed the dispute resolution—see Mattereum, for example. Each of the parties agreed with the process and arbitration board, and each party has a known identity, fulfilling KYC as part of onboarding.

- Accounting standards: What accounting standards does SweetBridge employ? SweetBridge proposes using an economy-level accounting system, based on International Financial Accounting Standards (IFRS) and Generally Accepted Accounting Principles (GAAP) rules. These are established rules, well deployed and well understood—covering business purposes and transaction types. SweetBridge is also working with regulatory bodies to have digital assets treated as cash equivalents, such as stable-coins over time.

PRESENTATION ON SUPPLY CHAINS IN INSURANCE INDUSTRY: RISK COOPERATIVE

Summary

The U.S. insurance industry is very "analog," a friction laden business model—and thus could benefit from the use of the supply chain of contracts based on blockchain technology. The industry is a very vertical industry with an expense ratio ranging between 30 and 50 percent, depending on the class of risk. As such, there is clearly a misaligned capital structure. This misalignment is exemplified by research that indicates that 40 percent of U.S. public is unable to tolerate a $400 setback. There is currently about $7 billion in unclaimed life insurance proceeds in the U.S., due to the burden of proof being placed on the claimants. This inefficiency could be addressed with better visibility, transparency, and security through the use of blockchain technology. The Edelman Trust Barometer indicates that today there is a record decline in both public and private institutional trust since the survey was started.

Currently there are efforts in the insurance industry to make use of blockchain technology to provide better visibility and transparency. Examples: R3's corda blockchain, the Institutes Risk Blocks Alliance and the B3i consortium, which is working with the reinsurance industry. Individual projects, like a blockchain-based risk registry, is being used to speed up response times to claims processing by allowing policyholders and insurers to catalogue coverage and share real-time information—in effect, beginning to address the "information asymmetry" problem. This is an important problem to address from the perspective of price discovery. The registry envisions the use of "smart" policies of all types, which will be stored on a blockchain and which automatically track premiums, pay claims, and keep records. The registry will also eliminate time-consuming audits by underwriters, because transactions will be visibly recorded on the blockchain.

Discussion Points (Q&A)

- Insurance obligations: A question from the audience—regarding experience with the Global Trade Digitization effort—noted that it was difficult to determine when one insurer's obligation stops and another's starts. Maersk is a great example of how that can work notionally but it depends on many participants to join into the system, which has approximately 1700 insurance rules. Disruption occurs when 10 times efficiency is achieved, so Maersk is able to use its purchasing power to make the industry process change. Indeed, some of the top insurers are starting to see that benefit and influencing process change.
- Regulation: Currently, regulation is a big friction point—state by state regulation is a major pain point causing friction in U.S. If there is an ask from the government, the insurance industry needs more liquidity, and there is currently a regulatory mismatch. The "suppliers of last resort," such as FEMA, have become the first resort in large losses, including flood, uninsured cyberattacks, among others. There needs to be a sandbox to explore a more

federated model of risk management. Exploration is needed in a crowdsourced model of capital, coming in from different parts of the world. We need a common harmonized regulatory framework.

PRESENTATION ON SUPPLY CHAIN OF GOODS: IBM

Summary

The presentation from IBM puts forward blockchain as a possible next generation infrastructure for tracking and fulfillment of goods or components in a partner ecosystem. Internally, IBM itself is developing solutions based on blockchain technology for (i) customs declaration management, (ii) assets management or the tracking of hardware components, and (iii) contracts labor management. A key driving factor is the need for better end-to-end supply chain visibility and better supply chain paperless trade. An example of better visibility is the successful United Postal Service (UPS) supply chain, a single entity. Similarly, Amazon can be successful because it is effectively a single supply chain owned by one entity. However, in a global supply chain, there are many participants and value must accrue to each member of the supply chain. As such, there is the additional need for balance between data visibility and data segmentation visible only to relevant parties. Smart contracts technology can provide the controls regarding who gets to see what data and when.

IBM is working with key players in the global supply chains industry to introduce blockchain technology as the next generation infrastructure of supply chain management. An example of this effort is the Global Trade Digitization project by IBM, Maersk, and other entities. The digitalization of customs declarations and the use of IBM blockchain allows these forms to be tracked and verified globally by all parties in the supply chain. This effort provides a potential cost savings of 10 percent—or roughly $1.8 trillion annually.

Another blockchain related project from IBM is focusing on the supply chain of medical goods and pharmaceuticals. Aside from tracking pharmaceuticals through the supply chain, the use of advanced chemical spectral analysis—of the surface of tablets and pills—allows for the detection of counterfeit pharmaceutical goods.

Discussion Points (Q&A)

- What is the ask from the Government: Accept, as legally valid, digital documents that are hashed-and-signed onto a blockchain. This would allow these documents (e.g., customs declarations) to have legal enforceability across jurisdictions. In turn, this would incentivize partners in the supply chain ecosystem to move to a shared blockchain system.
- Is the drug-counterfeit detection project using blockchain: The IBM project on fighting counterfeit drugs is in early stage and is investigating an easy-to-deploy solution to allow anyone to detect suspect pharmaceutical products. The approach uses a snap on lens on a mobile phone camera to zoom into the details of a given tablet or substance, coupled with strong analytics engine in the app. Thus, the user can obtain an immediate indicator as to the status of the pharmaceutical product. This is then tied to the pharmaceutical supply-chain system that runs on Hyperledger Fabric. The goal is to be able to track every legitimate pharmaceutical product from the point of production, to shipment and to arrival at the intended destination.

PRESENTATION ON SECURE SUPPLY CHAIN OF TRUSTED COMPONENTS: SEAGATE

Summary

The presentation from Seagate focuses on the supply chain of trustworthy hardware and software components that are increasingly crucial in certain markets, such as the federal government, military procurement, and certain categories of corporate IT environments. Seagate has been pioneering edge security and trustworthy computing since 2007. Currently, the electronics industry needs a new approach to provide "certification at the edge," and a large part of this is the need for "authenticating the physical to the digital." That is, how do we establish the provenance of a device—such as a disk drive—from the physical world as it enters deployment into the digital world and provides the infrastructure component for the digital world. Because Seagate is an international company, the various international data laws and privacy requirements will influence how products are developed.

As a use case example, currently Seagate provides Return Merchandise Authorization (RMA) services where hundreds of thousands of disk drives may be returned to Seagate and be redeployed in a new environment. A key requirement prior to redeployment is the assurance that a disk drive has been erased correctly, following not only verifiable processes but also in compliance to regulations in the country of deployment. This erasure is performed to ensure that data belonging to the original owner is truly deleted, and that "unprocessed" disk drives are not shipped out by mistake. A related aspect to this is the assurance that a disk drive branded Seagate is not a counterfeit disk drive, thereby harming the buyer.

Seagate already operates a certification process for RMA disk drives, but is currently exploring the use of blockchain technology to (a) record the certification status of each disk drive, (b) use the blockchain as a global medium in which the buyer can easy check the blockchain for the originality of a drive and make sure it is not counterfeit, and (c) ensure that if the drive has undergone RMA, there is a certification that can be tracked via the blockchain. The blockchain supports counterfeit detection/prevention by recording the digital identity of physical device at initial design and manufacturing. Aside from GDPR compliance, this provides a way to bridge Seagate and its customers by providing validated authenticity in warranty devices. The overall benefits increased trust, increased operational efficiency, and assured product and component authenticity, which in turn reduces the cost of business for Seagate.

Discussion Points (Q&A)

- What are the challenges: For the blockchain-based approach to succeed, other components suppliers, from PC component makers and OEMs, must be willing to join the ecosystem/network. Other challenges are customer and market pull, and the question as to who pays for blockchain infrastructure. Aside from the blockchain aspect, there are challenges as to whether the technology industry is ready—are processes mature? It's a question of architecture integration, from edge to core, and whether the ecosystem enables or prohibits innovation.
- What is the ask from the government: The ask is for the U.S. government to enforce its own regulations with regards to cybersecurity laws and standards, and to stop issuing "waivers" for suppliers who do not meet these standards, such as the Lowest Price Technically Acceptable (LPTA). There is concern that this has long-term negative impact on the U.S. cyber-infrastructure as a whole.

PRESENTATION ON A DECENTRALIZED CULTURE: U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Summary

The presentation from HHS addressed the question of how we can decentralize business processes in such a way that creates culture in which that our people want to operate. As example, currently HSS has to deal with 40 different systems that together manage expenditures of up to $6 billion. Much of the current business processes still rely on "semi-manual" use of inappropriate tools, such as Microsoft Word, Excel, etc.

One key aspect is the control of data pertaining to these transactions. The current predominant model is one where HHS has to deal with numerous suppliers, each with its own application programming interfaces (APIs) and each holding data that is relevant to the operations of the HHS. In effect, these suppliers are "in the driving seat" of the business process of the HHS, by way of each supplier holding a slice of the "view" of the whole business process.

The HSS since last year has explored low cost approaches by combining the use of (a) cloud computing capabilities, with (b) microservices operated by HHS, and (c) blockchain using Hyperledger Fabrics to track the status of these business processes. This is built over the existing system and does not impact the operations of this existing system in any way. The ultimate goal is to rebuild the way public procurement is done.

For example, if a supplier or other part of the government wishes to interact with HHS, they can now do so through the microservices at the HHS, with the microservices accessing the relevant data within the boundaries of the HHS infrastructure. The net result is that HHS remains in control of all parts of its data, that HHS no longer has to use the numerous APIs of the suppliers, and thereby rebalancing correctly the relationship between HSS and its suppliers. Using this architecture approach, HHS implemented five contracting systems—handling about one million contracts—using Hyperledger Fabric, with an analytics suite built using "soft AI" and process automation. This reduced the time for transaction completion from an average of 45 days to just a few minutes.

Related to this is the effort to develop a network of industry partners that can decentralize the orchestration layer by provisioning themselves the microservices initially obtained from HSS. This decentralized model seeks to allow simple questions/queries regarding pricing of computer parts to be answered in a few milliseconds in real-time—versus the old way of looking up huge Excel sheets. Thus, the use of (a)-(c) above allows for the automation of financial reviews also. The overall benefits include acquiring savings, reduction in work time/effort, and the shift from CapEx to OpEx. The use of a blockchain allows the HHS to avoid vendor lock-in, while at same time proving increased transparency and visibility.

Discussion Points (Q&A)

- How does this approach impact other federal agencies: The same approach via decentralized microservices and blockchain technology can be adopted by other agencies. One question is the push/pull approach with regards to data sharing. In either push/pull model, the key aspect is the decentralization of these services as a core part of the IT infrastructure.

- Internal resistance of upper management: There will be internal resistance if we just talk about it. The best way is to develop a low-cost functional proof of concept—one or two microservices—and show a working demonstration to leadership. Explaining how this decentralized model will positively impact business is more easily done with such a proof demo. As example, the project at HHS started in early January 2018 and was already completed by mid-April 2018. The cost was very low ($250,000), which means the project can be cancelled at any time without any financial impact. This low cost is negligible compared to the old way of procuring new services.
- What is the ask from government: Centralizing business processes is not the answer. It may work for a while for an individual agency or one industry partner, but it hurts the larger ecosystem as a whole. Empowerment of the CIO does not help because it becomes a centralizing process. It's better to drive value across agencies and providers, versus centralization to individual agencies and providers.

OPEN DISCUSSION

Challenges and Gaps with Widespread Use of Blockchain Technology

- Many states are creating theory own regulations, which is not good for business and innovation. The world is now a global environment and no single nation can control what happens. The U.S. has diminished powers to dictate. Regulatory bodies in each nation control or influence the competitiveness of that nation. For example, the total amount of Initial Coin Offerings (ICOs) worldwide was $16 billion in May of 2018, with only less that 22 percent in the U.S. Thus, the U.S. is losing the power of capital formation, which in the long term has dramatic negative impact on U.S. capital markets.
- The real power of blockchain technology is akin to "economic games," involving wealth creation and economic growth. There are many nations that wish to take away the leadership position away from the U.S. If the current trends continue, the U.S. will lose its digital-blockchain economics edge within 12 months, thus losing leadership in blockchain technology. One possible emergent leader could be the United Kingdom, because post-Brexit the UK is essentially a "burning platform." They have to do something drastic, or perish. UK businesses are investing heavily in digital-blockchain economics.
- The U.S. government needs to allow and promote exploratory work via sandboxes. An attendee opined that sandboxes are too late today, and that the U.S. government needs to do something drastic to make up for the loss of technology leadership. The U.S. government needs to delegate to industry due to this frightening pace of change, something that the government is not able to keep up with. The government need to "stop regulating technology" and look seriously into allowing for the adoption of virtual currencies and tokenization. Congress cannot stop agencies from issuing counter-productive rules.
- An attendee commented that currently there is no coherent thought/strategy across government on this space, and there is true lack of knowledge. There is no stated vision or mission from the government regarding this new digital-blockchain economics direction, and it is unclear who in government has this role. As comparison, in Singapore and UAE there has been a vision statement issued by their monetary authority. The emphasis is on "vision setting" not centralized control, because having one U.S. government agency "shaping" the narrative is also undesirable as it hinders true innovation.
- The moderator commented that DARPA invested hundreds of millions of dollars in the 1970s and 1980s, providing researchers with the freedom to innovate. The process took a long time but established the foundation of the architecture of the IP Internet today that

allows it to scale very well. What if DARPA or another government agency made mega-billions available to address the challenges of the new world of digital-blockchain economics, with the goal of keeping the U.S. at the forefront of this development?

- An attendee member suggested a comparison with the healthcare industry and pharma industry. Aside from HIPAA regulations needing to be updated, what would it take for these industries to move onto a supply-chain model based on blockchain technology? For example, how can the entire pharmaceutical lifecycle be developed over decentralized architectures and services based on blockchains? There was a general comment from an attendee that there needs to be more understanding among agencies on the nuances of blockchain, such as basic differences between blockchain technology as generic infrastructure versus Bitcoin as just one application of it.
- An attendee from New York commented that the New York Economic Development Corporation has opened up a blockchain resource center to educate state/local government regulators. The center will serve as a physical hub for the industry, with the goal of building public awareness of blockchain technology through education. It also wants to be a mechanism to connect entrepreneurs to business, and other entities in the ecosystem. This raised a question from another attendee, asking what municipalities could do in this innovation space.
- Another person raised the point that blockchain technology is a powerful positive catalyst for innovation, something that is rare in occurrence in the history of technology development. Other countries have picked up on this aspect. What is needed is a way to incentivize people through (i) positive communications on this matter on the part of the government, (ii) clear and unambiguous support for exploration through sandboxes, and (iii) positive economic incentives for people to succeed. The response from an attendee, a federal government person, is agreement and encouraged industry to do a better job at explaining the value proposition of digital-blockchain economics and the huge relevance it has for the future of the U.S. economy.
- An attendee floated the idea of the government establishing a commission for digital-blockchain economics and blockchain technology, similar to the commissions for artificial intelligence (HR5356/S2806) and for quantum computing.
- An attendee commented that the technology industry needs to clarify usage of the term "blockchain" and not use it when it is not appropriate. The industry needs to continue developing its storytelling by using the correct value proposition of blockchain technology. That is, it needs to reduce the hype because it is confusing many people, including those in leadership in government. Lawmakers need easily digestible examples of what blockchain is good for in order to make it consumer-accessible—as easy as explaining Uber or the iPhone. Another attendee commented that right now there are great use case pilots but there are still no production examples of blockchain technology for supply chains. Once these production examples exist, this enables lawmakers and agencies to expand on these successful examples. An attendee, from a federal agency, agrees with this last assertion, that once the agencies see the success path, and are properly educated, then they will pursue pushing for adoption of the technology. Another attendee, also from a federal agency, stated that involvement from NIST is very significant because it signals to government agencies that this technology is serious.
- An attendee commented that industry needs to work with federal agencies, beginning within existing frameworks of agencies and existing laws. This was followed by a comment that many agencies still operated using regulations on their books from 40 years ago, which did not contemplate new ways of technology, which includes of course blockchain. Industry needs to do a better job of explaining to government and regulators the value proposition of this new technology.

KEY CONTACT INFORMATION

To contact the author:

Thomas Hardjono
MIT Connection Science
77 Massachusetts Avenue E15-386
Cambridge, MA 02139
hardjono@mit.edu

REPORTS FROM THE IBM CENTER FOR THE BUSINESS OF GOVERNMENT

For a full listing of our publications, visit www.businessofgovernment.org

Recent reports available on the website include:

Acquisition

Ten Actions to Improve Inventory Management in Government: Lessons From VA Hospitals by Gilbert N. Nyaga, Gary J. Young, and George (Russ) Moran
Beyond Business as Usual: Improving Defense Acquisition through Better Buying Power by Zachary S. Huitink and David M. Van Slyke

Collaborating Across Boundaries

Cross-Agency Collaboration: A Case Study of Cross-Agency Priority Goals by John M. Kamensky
Interagency Performance Targets: A Case Study of New Zealand's Results Programme by Dr. Rodney Scott and Ross Boyd
Integrating and Analyzing Data Across Governments - the Key to 21st Century Security by Douglas Lute and Francis Taylor

Improving Performance

Seven Drivers Transforming Government by Dan Chenok, Haynes A. Cooney, John M. Kamensky, Michael J. Keegan, and Darcie Piechowski
Five Actions to Improve Military Hospital Performance by John Whitley
*A Framework for Improving Federal Program Management*by by Janet Weiss

Innovation

Tiered Evidence Grants - An Assessment of the Education Innovation and Research Program by Patrick Lester
A Playbook for CIO-Enabled Innovation in the Federal Government by Gregory S. Dawson and James S. Denford
Making Open Innovation Ecosystems Work: Case Studies in Healthcare by Donald E. Wynn, Jr., Renée M. E. Pratt, and Randy V. Bradley
Laboratories of Innovation: Building and Using Evidence in Charter Schools by Patrick Lester within "Innovation"

Leadership

Best Practices for Succession Planning in Federal Government STEMM Positions by Gina Scott Ligon, JoDee Friedly, and Victoria Kennel

Risk

Risk Management and Reducing Improper Payments: A Case Study of the U.S. Department of Labor by Dr. Robert Greer and Justin B. Bullock
Ten Recommendations for Managing Organizational Integrity Risks by Anthony D. Molina
Managing Cybersecurity Risk in Government by Rajni Goel, James Haddow and Anupam Kumar

Using Technology

Delivering Artificial Intelligence in Government: Challenges and Opportunities by Kevin C. Desouza
Using Artificial Intelligence to Transform Government by The IBM Center for The Business of Government and the Partnership for Public Service
Digital Service Teams: Challenges and Recommendations for Government by Professor Dr. Ines Mergel
Ten Actions to Implement Big Data Initiatives: A Study of 65 Cities by Alfred T. Ho and Bo McCall
A Roadmap for IT Modernization in Government by Dr. Gregory S. Dawson

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, DC 20005
202-551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:

or, send us your name and e-mail to receive our newsletters.

IBM Center for
The Business of Government
20 years of research for government:
informing today, envisioning tomorrow
1998-2018