Testimony of

Douglas Maughan
Division Director
Science and Technology
U.S. Department of Homeland Security
Before the
Committee on Science, Space, and Technology
Subcommittee on Oversight
Subcommittee on Research and Technology

May 8, 2018

Chairman Abraham, Chairwoman Comstock, Ranking Member Beyer, Ranking Member Lipinski and distinguished members of the Oversight and Research and Technology Subcommittees, thank you for inviting DHS to speak with you today. I will be addressing the topic of "Potential and proven applications of blockchain and distributed ledger technology in shipping, logistics, and customs, with an emphasis on supply chain management" and sharing with you important aspects of how we are exploring the use of blockchain and distributed ledger technologies in research and development and working with several DHS mission areas to integrate innovative technology into everyday use.

I have been in the Science and Technology Directorate (S&T) for 14.5 years working the entire time on Cybersecurity research and development (R&D). Prior to my time at DHS, I worked at the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency and have been involved in cybersecurity R&D as a government employee for over 30 years.

As the R&D arm of DHS, S&T develops the tools, technologies, and knowledge products for DHS operators, state and local first responders, and the nation's critical infrastructure, ensuring R&D coordination across the Department to develop solutions for the needs of today and tomorrow. S&T partners with Federal agencies, industry, academia, and international governments to create and test solutions that help the nation's homeland security officials prevent, respond to, and recover from all hazards and threats. S&T's goal is to provide real-world solutions in a realistic timeframe.

The Benefits and Opportunities of Blockchains

Blockchains offer much promise, as can be seen in the rapid growth of interest across government and the private sector. From a government perspective, the technology holds the potential for enhanced transparency and auditing of public service operations, greater supply chain visibility to combat the distribution of counterfeit products, and automation of paper-based processes to improve delivery of services to organizations and citizens. Examples span the gamut from ensuring the authenticity and integrity of videos and photos from cameras, sensors and Internet of Things (IoT) devices; enhancing and facilitating international trade and customs

processes; facilitating and securing international passenger processing; to mitigating forgery and counterfeiting of official licenses and certificates.

Conversely, the challenge with blockchain technology is the potential for the development of "walled gardens" or closed technology platforms that do not support common standards for security, privacy, and data exchange. This would limit the growth and availability of a competitive marketplace of diverse, interoperable solutions for government and industry to draw upon to deliver cost effective and innovative services based on blockchain and distributed ledger technologies.

From the DHS S&T perspective, this is the trajectory we see for the blockchain and distributed ledger technologies in the near future:

(A) Awareness of blockchain and its potential is increasingly becoming part of the mainstream business and government discussion. Fueled by promise, publicity, marketing, and market investment, organizations are looking for vendor-neutral guidance and best practices on when, where, why, and how this technology can be used. Such unbiased knowledge and implementation expertise is in very short supply, which will likely have significant impact on adoption.

(B) The lack of best practices and implementation design patterns leads to knowledge and action asymmetries. In the race to achieve technological advantage and market share, decision criteria to evaluate the appropriate blockchain technologies are indeed appropriate for a particular situation are neglected. There are many types of blockchains with varying degrees of support of classic security principles such as confidentiality, integrity, and availability as well as support of privacy principles such as pseudonymity and selective disclosure. Analysis to determine if a particular blockchain supports these security and privacy considerations is either non-existent or not readily available.

(C) There is an increasing tension between business/system owners, both in the private sector and public sector, and their technology and solution providers. For example, a technology provider's desire to gain traction for their particular blockchain implementation may run up against the business/system owner's expectation of having an open architecture environment for their systems, rather than vendor-specific approaches to prevent technology lock-in. Technology providers may recommend a replacement strategy to implement their blockchain, which runs counter to the business/system owners desire for new technology to integrate with their current business processes and technology to preserve and leverage existing investments.

(D) Private industry is leading the way in blockchain development, as many see implementing blockchain as a key competitive advantage. The private sector's significant investments and the ability to adopt technologies and processes faster than the public sector presents the government with a key decision point on how to best participate in this growing, but still nascent field. Government must be informed and ensure blockchain technology -- as it evolves -- supports standardized approaches for security, privacy, and data exchange to create efficiencies and enhance the public good. Government must also

consider leadership opportunities within the broader community and partner with industry to bring solutions to market.

DHS S&T and Blockchain

As the Science Advisor and the R&D arm of the Department, supporting the needs of our operational components is among our highest priorities. DHS S&T's decision approximately three years ago to start evaluating the security and privacy implications of blockchain technologies as well as our funding and involvement in the technical work since that time has resulted in placing our emphasis on architecture, standards, and interoperability and has allowed us to bring a level of rigor, expertise, and credibility that is unique in supporting DHS Components and other partners across the U.S. government.

Blockchain technologies are an integral part of several ongoing S&T research projects with DHS Components and other partners for a variety of purposes, including: developing best practices and decision criteria on when and how to implement blockchain technologies; understanding the support for security and privacy principles in commercial blockchain implementations; developing a decentralized identity broker that separates authentication and attestation services; learning about best practices for connecting legacy systems with blockchain enabled capabilities; developing specifications to ensure standardized approaches for decentralized identifiers; interoperable data formats using verifiable credentials and scalable and usable approaches to decentralized key management systems. These specifications, which are or will be submitted by S&T performers to global standards organizations to undergo an open, multi-stakeholder standardization process, are open, royalty-free, and free to implement, and are accompanied by implementation lessons to demonstrate their utility.

S&T Engaging CBP

Within DHS, U.S. Customs and Border Protection (CBP) has been the most active operational component to lean forward in partnering with S&T on exploring the use of blockchain and distributed ledger technologies for its mission. Our ongoing engagements with CBP include:

- Proof of concept deployments with the U.S. Border Patrol to evaluate how blockchain technology can be used to ensure the imagery and sensor data from cameras, fixed and mobile, can be ensured for authenticity and integrity.
- Conducting analysis of alternatives and blockchain technology feasibility explorations with the CBP and others to understand the potential benefits and challenges in using blockchain technology for enhancing and facilitating international passenger travel.
- Conducting proof of concepts deployments in partnership with CBP's Office of Trade and Office of Trade Relations that are directly focused on applications of blockchain and distributed ledger technology to shipping, logistics, and customs by providing visibility into globally distributed supply chains to help facilitate the movement of legitimate goods while combating the distribution of counterfeit goods.

A good example for a proof of concept effort with CBP on imagery and sensors involves the Internet of Things (IoT) Security. Based on CBP's technical requirements S&T engaged an Austin, Texas startup company, via the DHS Silicon Valley Innovation Program. This project captured and made clear the architecture choices and design decisions inherent in building an immutable record of data coming from cameras, sensors and IoT devices. It resulted in lessons

learned regarding the key issues that exist when integrating new technologies with existing government business and technical processes and the choices needed to ensure that private data should not be resident on a public blockchain while enabling the ability to publically validate the private data. S&T conducts its projects over multiple phases to minimize project and technical risk and this project is beginning deployment in an operational environment in partnership with CBP.

Blockchain Technology and Trade

DHS S&T, CBP Office of Trade (OT), and CBP Office of Trade Relations (OTR) are working together with private sector members of the Emerging Technologies Working Group of the CBP Commercial Customs Operations Advisory Committee (COAC) on multiple proof-of-concept implementations to identify the utility and feasibility of blockchain technology. DHS S&T conducted a two-day workshop with the COAC industry partners to provide information to the participants so that they are able to actively engage in the discussions about blockchain use with CBP. Included in the workshop was the development of a shared set of criteria to be used to evaluate the proof-of-concepts S&T and CBP (OT and OTR) would embark upon. Those criteria included:

- Use of an existing business process rather than creating something new.
- Ability to define metrics related to the existing business processes to ensure that the development of new technologies can be measured against existing metrics as a success criterion.
- Ability to run the blockchain enabled business process in parallel with existing business processes (A/B Testing).
- Needs to benefit a broad range of stakeholders.
- Must involve multiple roles and information sharing with differing parties who do not wish to have a shared infrastructure.
- Defined data model for data to be shared.
- Lessons learned to inform programs, requirements or regulations.

Using this criterion to walk through the various use cases of interest, resulted in a prioritized list of potential proof-of-concepts. We are currently executing the highest priority one which is to track free trade qualifications of imported goods by providing greater supply chain visibility, which would answer the following question, “Can distributed ledger technology be used to verify that an item qualifies for a free trade import tax exemption by demonstrating that the necessary percentage of an item’s components were produced/assembled in a FTA country?” For this first Customs use-case, we are currently in the proof-of-concept phase with a Blacksburg, Virginia company. It is testing certificates associated with two particular Free Trade Agreements: the North American Free Trade Agreement (NAFTA) and the Central America Free Trade Agreement (CAFTA). Recently, S&T and CBP provided a 2-day exchange meeting into the technical requirements with the various trade and policy groups. The project has transitioned from the operational design phase to the technical requirements development and testing phase. There will be careful analysis of the success metrics at the end of this phase that will result in a GO/No-Go decision for the next phase.

Flexible Ledgers with Verifiable Credentials, Blacksburg, VA company

This project designed and implemented a generalized, configurable ledger technology that can support application specific needs while using a standardized, extensible core data model to ensure interoperability. It has resulted in a commercially available capability that incorporates interoperability specifications such as DIDs and Verifiable Credentials which are both on the standardization path via the World Wide Web Consortium (W3C). Given its support for these specifications, this technology is being used by the DHS/CBP Office of Trade in partnership with S&T for its first customs proof-of-concept.

Additional Blockchain Projects

In addition to work with DHS/CBP, S&T has contributed to the following efforts that have influenced and informed our supply chain focused blockchain work:

Decentralized Identifiers (DIDs), Seattle, WA company

Developed a decentralized identifier (DID) specification that enables the creation of a globally unique identifier without the need for a central registration authority. This identifier should be immutable, globally resolvable and cryptographically verifiable. At the end of this project a draft specification was developed and the Seattle, WA company was acquired by a Herriman, UT company.

Decentralized Key Management System (DKMS), Herriman, UT company

Using the DID specification developed by Respect Network Corporation, designed, developed and implemented a decentralized key management capability that is compatible with the requirements of the National Institute of Standards and Technology (NIST) 800-130 Cryptographic Key Management System Framework. Currently, the results of this work which includes the NIST 800-130 analysis as well as the architecture and design of the DKMS system is complete and has contributed to the open source Hyperledger Indy project (led by the Linux Foundation) for public review and comment. Next steps include a reference implementation as well as further test and evaluation based on community feedback.

Decentralized Identity Broker, Toronto, Canada company

This project designed, developed and implemented a decentralized identity broker that separates authentication and attestation services while ensuring resiliency against denial of service attacks, preventing honeypots of data, providing citizen centric consent and control of data sharing, while supporting international standards for identity assurance, privacy and data sharing. It has resulted in a commercially available capability that utilizes the Hyperledger Fabric project (also led by the Linux Foundation) that is currently undergoing operational testing in preparation for production deployment in the U.S. market.

A Path Forward

As noted before, a very real concern in the current timeframe of blockchain technologies is the potential for the development of “walled gardens” or closed technology platforms that do not support common standards for security, privacy, and data exchange. This would limit the growth

and availability of a competitive marketplace of diverse, interoperable solutions for government and industry to draw upon to deliver cost effective and innovative services based on blockchain and distributed ledger technologies.

To that end, DHS S&T is pursuing two broad courses of action to encourage a more open and inclusive future for blockchain technology:

1. Support development of globally available specifications (precursor to standards) that are open, royalty free, and free to implement to ensure interoperability across systems while ensuring there is no vendor lock-in.
    a. Decentralized Identifiers (DIDs) via World Wide Web Consortium (W3C) Standardization Process
    b. Verifiable Claims Data Model via W3C Standardization Process
    c. Decentralized Key Management System via TBD (Potentially OASIS)
2. Actively work with and support our DHS Component customers, such as CBP, to understand their potential use cases for blockchain and help them achieve their outcomes with the needed R&D expertise and technologies.

We believe that our careful and considered approach benefits not just us but everyone who is considering the use of a blockchain technology in the long term by ensuring there is no vendor lock-in and there are multiple vendors with interoperable solutions from which we can buy.

Summary

Chairman Abraham, Chairwoman Comstock, Ranking Member Beyer, Ranking Member Lipinski, and distinguished members of the Oversight and Research and Technology Subcommittees, thank you again for your interest in blockchain or distributed ledger technologies and how these technologies will help DHS accomplish its important mission areas.

DHS S&T is focused on applied R&D of technologies with critical significance to DHS Components and other key parts of the Homeland Security Enterprise. Blockchain and distributed ledger technologies are rapidly moving from hype to reality in application domain areas where DHS S&T is currently working. This reality means DHS S&T must aggressively work with its research, development, test and evaluation partners throughout government and industry so homeland security applications of blockchain and distributed ledger technology are effective and trusted. This requirement includes strong working relationships with industry, so homeland security applications can leverage the best of industrial innovation, and homeland security capabilities can continue to support the strengthening and growth of American economic capabilities. These efforts must contribute to key challenge areas for all critical missions of DHS.

Thank you for your thoughtful leadership on these issues. I look forward to your questions.

APPENDIX: Selected References Blockchain and Distributed Ledger Technologies

Decentralized Identifier Primer, GitHub.com, October, 2017, https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/draft-documents/did-primer.md.

A Verifiable Claims Primer, GitHub.com, October 2017, https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/draft-documents/verifiable-claims-primer.md.

DKMS (Decentralized Key Management System) Design and Architecture V3, GitHub.com, April 12, 1018, https://github.com/hyperledger/indy-sdk/blob/master/doc/dkms/DKMS%20Design%20and%20Architecture%20V3.md.

NISTIR 8202 (DRAFT) - Blockchain Technology Overview, https://csrc.nist.gov/publications/detail/nistir/8202/draft

Homeland Security

Biography

W. Douglas Maughan, Ph.D.

Director, Cyber Security Division

Science and Technology Directorate

Dr. Douglas Maughan is the Division Director of the Cyber Security Division in the Homeland Security Advanced Research Projects Agency (HSARPA) within the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS). Dr. Maughan has been at DHS since October 2003 and is directing and managing the Cyber Security Research and Development activities and staff at DHS S&T. His research interests and related programs are in the areas of networking and information assurance. Dr. Maughan has been responsible for helping bring to market over 40 commercial and open-source information security products during the past 12+ years while at DHS and is the Senior Executive responsible for the DHS Silicon Valley Innovation Program.

Prior to his appointment at DHS, Dr. Maughan was a Program Manager at the Defense Advanced Research Projects Agency (DARPA). Prior to his appointment at DARPA, Dr. Maughan worked for the National Security Agency (NSA) as a senior computer scientist and led several research teams performing network security research.

Dr. Maughan received Bachelor's Degrees in Computer Science and Applied Statistics from Utah State University, a Masters degree in Computer Science from Johns Hopkins University, and a PhD in Computer Science from the University of Maryland, Baltimore County (UMBC).

# # #