Testimony of

Charles H. Romine, Ph.D.
Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the

United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight
and
Subcommittee on Research and Technology

"Beyond Bitcoin: Emerging Applications for Blockchain Technology"

February 14, 2018

Introduction

Chairman Abraham, Ranking Member Beyer, Chairwoman Comstock, Ranking Member Lipinski and members of the Subcommittee, I am Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in cybersecurity and blockchain.

The Role of NIST in Cybersecurity

With programs focused on national priorities, from advanced manufacturing and the digital economy to precision metrology, quantum science, and biosciences, NIST's overall mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, starting with the development of the Data Encryption Standard, when the potential commercial benefit of this technology became clear. NIST's role, to research, develop, and deploy information security standards and technology to protect the Federal Government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA 2002) (Public Law 107-347[1]), and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST standards and guidelines are developed in an open, transparent, and collaborative manner that enlists broad expertise from around the world. While developed for federal agency use, these resources are often voluntarily adopted by other organizations, including small and medium-sized businesses, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective and accepted globally. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

Blockchain

Blockchains are immutable digital ledger systems implemented in a distributed fashion—that is, without a central repository—and usually without a central authority. At their most basic level, they enable a community of users to record transactions in a ledger that is public to that

[1] FISMA 2002 was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347; 116 Stat. 2899).

community, so that transactions cannot be changed, once published, without the community knowing.

These transactions are secured with cryptographic hashes, and transactions are signed and verified using public/private key pairs. The transaction history is summarized to efficiently and securely record a chain of events so that any attempt to edit or change a past transaction requires all subsequent blocks of transactions to be recalculated.

In 2008, the blockchain idea was combined in an innovative way with several other technologies and computing concepts to enable the creation of modern cryptocurrencies, which are electronic money protected through cryptographic mechanisms instead of a central repository. The first such blockchain-based approach was Bitcoin, followed by Ethereum, Ripple, and Litecoin. As a result, blockchains are often viewed as synonymous with Bitcoin or possibly e-currency solutions in general, but its applications are broader than fund transfer security.

Currency blockchain systems are novel because they store value, not just information. The value is attached to a digital wallet—an electronic device or software that allows an individual to make electronic transactions. The wallets are used to sign transactions sent from one wallet to another, to record the transferred value publicly, and to allow all participants in the network to independently verify the validity of the transactions. Each participant can keep a full record of all transactions, making the network resilient to attempts to alter that record or forge transactions later.

Many electronic cash schemes existed prior to Bitcoin, but none of them were widely used. By adopting blockchain technology, Bitcoin achieved compelling capabilities that promoted its use. The use of a blockchain enabled Bitcoin to be implemented in a distributed fashion so that no single user controlled the currency and no single point of failure existed. Bitcoin's primary benefit is to enable direct electronic financial transactions between users without the need for a third party.

By using a distributed blockchain and consensus-based maintenance, a self-policing mechanism was created, ensuring that only valid transactions are added to the blockchain. Blockchain enables users to be pseudonymous, meaning that the identity of the users is anonymous but their accounts are not—all their transactions could be seen publicly. Also, the distributed maintenance of the blockchain created a completely transparent system, which promoted trust in its use. Blockchain use cases vary from banking to supply chain to insurance and healthcare.

The use of blockchain technology, however, is not a silver bullet. Some issues must be considered, such as how to deal with malicious users, how controls are applied, and the limitations of any blockchain implementation. Once a blockchain is implemented and widely adopted, it becomes very difficult to change it. Once something is recorded in a blockchain, it is usually there forever, and it takes a significant effort—involving a majority of the community—to make a change, even when there is a mistake.

NIST Activities Related to Blockchain

Blockchains use well-known computer science mechanisms (such as linked lists and distributed networking) and cryptographic primitives (such as hashing, digital signatures, and public/private keys) mixed with financial concepts (such as ledgers). NIST has a strong research program in advancing measurement science for computer security, cryptography, and cryptographic key management.

In January 2018, NIST published draft NIST Internal Report 8202 "Blockchain Technology Overview.[2]" The report describes how a blockchain system works and provides a common language for communication among technology developers and users. Organizations considering implementing blockchain technology need to understand important aspects of the technology, and users of this technology need to understand its advantages and disadvantages.

NIST collaborates with experts from industry, academia, and government to strengthen its research portfolio and to create and promote solutions to real-world problems. In September 2017, NIST and the Office of the National Coordinator for Health Information Technology cohosted an industry-wide workshop titled "Use of Blockchain for Healthcare and Research."

On September 18 and 19, 2018, NIST will host the Institute of Electrical and Electronics Engineers (IEEE) Blockchain Summit at its campus in Gaithersburg, Maryland. Researchers and developers from industry and academia will share insights on the status of current usage studies, where new opportunities are surfacing, and critical questions and challenges that need to be addressed to advance blockchain technology.

Cryptography

NIST has conducted extensive research activities on asymmetric-key cryptography, also referred to as public/private key cryptography, a fundamental technology utilized by blockchain technologies. Asymmetric-key cryptography uses a pair of keys—a public key and a private key – that are mathematically related to each other. For Federal information systems, Federal Information Processing Standard (FIPS) Publication 186-4, Digital Signature Standard,[3][4] specifies the Elliptic Curve Digital Signature Algorithm, which is a common algorithm for digital signing used in blockchain technologies.

A private key is usually generated using a secure random function, meaning that reconstructing it is difficult, if not impossible. NIST develops, maintains, and tests implementations that meet NIST's standards and guidelines for key generation and derivation, key establishment, and key exchanges.

---

[2] https://csrc.nist.gov/publications/detail/nistir/8202/draft

[3] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 186-4, Digital Signature Standard, July

[4] . https://doi.org/10.6028/NIST.FIPS.186-4

Because blockchains are not centralized, there is no intrinsic central place for user key management. Users must manage their own private keys, and if one is lost, anything related to that private key—such as digital assets—is also lost. There is no "forgot my password" or "recover my account" feature for blockchain systems. If a private key is stolen, the attacker will have full access to all assets controlled by that private key. The security of private keys is so important that many users rely on secure hardware to store them. When the news media announce that "Bitcoin has been reported stolen," it almost certainly means that the owner's private keys were found and used without permission to sign a transaction sending the money to a new account, not that the system was compromised.

Quantum Computing

The public key cryptographic algorithms used within most blockchain technologies for public/private key pairs will need to be replaced when powerful quantum computers become a reality. It is generally accepted that algorithms that rely on the computational complexity of integer factorization—or work on solving discrete logarithms—will be susceptible to quantum computing. NIST Internal Report 8105, titled "Report on Post-Quantum Cryptography,[5]" describes the impact of quantum computing on common cryptographic algorithms. NIST is currently working on developing, identifying, and selecting the next set of public key cryptography that will be effective when quantum computers come into use. NIST is leading this global effort, which aims to ensure this encryption is available to industry and built into products before quantum computers emerge.

Hash Functions

An important component of blockchain technology is the use of cryptographic hash functions. Blockchain technologies take a list of transactions and create a hash "fingerprint" for the list. Anyone with the same list of transactions can generate the exact same fingerprint. If a single value in a transaction within the list changes, the digest for that block changes, making it easy to discover even minor one-bit changes. Common hashing algorithms used by Bitcoin, Ethereum, and Litecoin are described in FIPS 180-4[6] and FIPS 202[7]. Also, the NIST Secure Hashing website[7] contains FIPS specifications for Federal information systems for all NIST-approved hashing algorithms.

NIST Blockchain Workbench

Research in how to more generally use blockchain platforms is hampered by high entry barriers, mainly resulting from the lack of training material, tools, and testbeds. NIST has developed a

---

[5] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[6] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 180-4, Secure Hash Standard (SHS), August 2015. https://doi.org/10.6028/NIST.FIPS.180-4

[7] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication SHA-3 Standard: Permutation-Based Hash and ExtendableOutput Functions, May 2014. https://csrc.nist.gov/csrc/media/publications/fips/202/final/documents/fips_202_draft.pdf [7] National Institute of Standards and Technology (NIST), Secure Hashing website, https://csrc.nist.gov/projects/hash-functions

blockchain workbench capability, which provides flexible testbeds and workbenches that NIST researchers can use to implement theoretical solutions. This capability also enables researchers to evaluate the potential usefulness of blockchain architectures for various applications. This distributed system is implemented on several servers, provides a graphical user interface, and is supporting a wide range of experimental scenarios developed by NIST. This hands-on experience is essential to complement NIST interactions with industry, as well as NIST research leading to reports, guidance, tools, and references.

NIST Participation in Blockchain Standardization

Under the provisions of the National Technology Transfer and Advancement Act (PL 104-113) and Office of Management and Budget (OMB) Circular A-119[8], NIST is tasked with the role of encouraging and coordinating federal agency use of voluntary consensus standards in lieu of government unique standards, and federal agency participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies to coordinate standards issues and priorities with the private sector through consensus standards developing organizations (SDOs), such as the InterNational Committee for Information Technology Standards (INCITS), Joint Technical Committee 1 of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), the Organization for the Advancement of Structured Information Standards (OASIS), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and other standards organizations such as the International Civil Aviation Organization (ICAO) and the International Telecommunication Union's Standardization Sector (ITU-T). NIST leads national and international consensus standards activities in biometrics, cryptography, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing—all of which are essential to accelerate the development and deployment of information and communication systems that are interoperable, reliable, secure, and usable.

Voluntary Consensus Standards

Most SDOs are industry-led private sector organizations. Many voluntary consensus standards from those SDOs are appropriate or adaptable for the U.S. Government's purposes. OMB Circular A-119 directs the use of such standards by U.S. Government Agencies, whenever practicable and appropriate, to achieve the following goals:

- eliminating the cost to the Federal Government of developing its own standards and decreasing the cost of goods procured and the burden of complying with agency regulation;
- providing incentives and opportunities to establish standards that serve national needs, encouraging long-term growth for U.S. enterprises and promoting efficiency, economic competition, and trade; and
- furthering the reliance upon private sector expertise to supply the Federal Government with cost-efficient goods and services.

[8] ''Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities,'' https://www.gpo.gov/fdsys/pkg/FR-2016-01-27/pdf/201601606.pdf

When properly conducted, standards development can result in increased productivity and efficiency in government and industry, greater innovation and competition, more opportunities for international trade, conservation of resources, increased benefits and choices for consumers, and improved health and safety.

In the area of blockchain standardization, NIST is actively participating in consensus-based, documentary standard development efforts at both national and international levels. For example, NIST participates in Accredited Standards Committee X9 (ASC X9) and INCITS, and will participate in the newly formed IEEE blockchain initiative. NIST participates as well in ISO Technical Committee 307 – Blockchain and Distributed Ledger Technologies.

Potential and Emerging Applications of Blockchain Technology

While financial organizations are likely to be the businesses most impacted by blockchains, many potential uses and opportunities for blockchain technologies exist beyond digital currency. For example, companies that need to maintain public records, such as holding a land title, marriage certificates, or birth records, can take full advantage of blockchains.

Blockchains also have strong potential for storing and recording supply chain records. A blockchain can record each step in a product's life: when it was created in a factory; when it was shipped and subsequently delivered to a store; and when a consumer purchased it.

New industries may also benefit from blockchain. Such industries include digital notaries seeking to prove that a person accessed a specific piece of information by recording its hash into the blockchain.

Conclusion

Blockchains are exciting technologies that have the potential to address real corporate and consumer needs using a strong and verified trust model. Much work still needs to be done to understand this technology, bring out its potential, and set the stage for markets to reward usable and secure implementations that meet real customer needs.

NIST will continue its research and development in the foundational cryptography that blockchains use. We will continue to learn from our research and continue to build collaborations with industry in the publication of guidelines. NIST is also continuing to work with international standards bodies that have started study groups and technical committees to initiate standards work for blockchains. This is an exciting time for blockchain technology, as it emerges into markets and sectors.

Thank you for the opportunity to testify on NIST's work regarding blockchain. I will be pleased to answer any questions you may have.