ASC X9 Study Group Report

Distributed Ledger and Blockchain Technology Study Group

A Study Group Report prepared and released by:
Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Release Date: April 6, 2018

THIS PAGE INTENTIONALLY LEFT BLANK

.

Contents

Page

Tables

Figures

Foreword

This document is not an American National Standard and the material contained herein is not normative in nature. Comments on the content of this document should be sent to: Attn: Executive Director, Accredited Standards Committee X9, Inc., 275 West Street, Suite 107, Annapolis, MD 21401,

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Introduction

Distributed ledger technologies and associated applications are beginning to make inroads in the financial services industry. The best known implementation, the Bitcoin blockchain, has been described as a "trustless" network that enables value transfer among participants without the need for an intermediary or central verifier. This innovation has been used to distribute new digital currency that is accepted for real world goods and services. While digital currency itself may be transformative where it is adopted, distributed ledger technologies, and in particular the main innovation of Bitcoin, the blockchain, extends into many other use cases that traditionally rely on third-party transaction verifiers: payments, audit, brokerage, asset registry, and more. Nearly all large financial institutions today are exploring applications of blockchain and other distributed ledger technology (DLT). Moreover, many financial industry and technology firms are joining together to explore the benefits of distributed ledgers delivered with blockchain technology.

In early 2016, R3 CEV (a consortium of international financial institutions) announced successful completion of experiments to transfer value across separate ledgers. Similarly, the Linux Foundation launched the Hyperledger Project in order to build an open source foundation for distributed ledger applications. As these efforts demonstrate, appetite exists for cooperation across industries. The development of standards could facilitate inter-operable, accessible solutions and accelerate innovation and adoption. Other experts have reached similar conclusions.[1]

Benefit of Standards

Standards can play several key roles in technology development. They can accelerate broader development and adoption by allowing innovators to work independently while maintaining interoperability. They can help ensure the quality and security of a solution by offering proven steps to eliminate or minimize potential weaknesses and ultimately protect consumers and businesses from common vulnerabilities. For emerging technologies, standards can create a marketplace for common and fully integrated applications.

The Study Group has concluded that Standards work specific to blockchain and distributed ledger technology is warranted because of several factors:

1. Distributed ledger technology includes common elements that may benefit from standardization to enable interoperable security, smart contracts, value transfer, etc.
2. The benefits provided by distributed ledger's reduced frictions and shared accounting are best achieved through agreement to use a single distributed ledger or interoperable technology with characteristics that are commonly accepted by all participants. As most distributed ledger application development today is within individual company silos and consortiums, X9 is positioned to advance innovation by identifying the areas where standards and common architectures/practices support risk management that can benefit the financial services sector as it adopts blockchain technology.

---

[1] UK Government Chief Scientific Adviser - Distributed Ledger Technology: beyond block chain, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf and Depository Trust and Clearing Company – Embracing Disruption, http://www.dtcc.com/news/2016/january/25/new-dtcc-white-paper-calls-for-leveraging-distributed-ledger-technology.

3. In the absence of a coordinated standards effort, market driven projects in blockchain are likely to proceed in a fragmented way and not gain the benefits of foundational building blocks, harmonization, and coordination that standards could provide at this early stage.
4. A broad range of companies may benefit from distributed ledger standards as the technology is expected to introduce new efficiencies to many processes. Standards can ensure that the legal and regulatory risk requirements of the financial services are met.

Risks of Standardization

The Study Group recognized that there is a risk to requiring standardized implementations at this early stage of innovation. Some perfectly sound solutions are not standard for the industry (e.g. elliptic-curve is highly regarded as secure cryptography but is not yet included in catalogs of financial service standards) and so standards may deter the introduction of innovations that meet or exceed the criteria applied to existing standards. For this reason, it is important that standardization not hinder innovation or be seen as an enforced requirement that creates the need for revising existing functional solutions.

In addition, because of the rate of change, the maturation of each area may evolve at unpredictable rates. Frequent review of high or medium importance areas to determine when additional efforts to adapt or create new standards should begin is warranted. Where possible, we have suggested timeframes for this review.

Objective of the Study Group

The objective of this study group was to assemble a group of industry experts to assess what types of standards for DLT, and specifically blockchain, would benefit the financial services industry and support more effective adoption of this technology. The resulting report (this document) provides this assessment, and includes a glossary of terms. This Report was processed and approved by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Report does not necessarily imply that all the committee members voted for its approval.

At the time this Report was approved, the X9 Board of Directors had the following leaders and members:

Roy C. DeCicco, X9 Chairman
Angela Hendershott, X9 Vice Chairman
Steve Stevens, X9 Executive Director
Janet Busch, Program Manager

Organization Represented on the X9 Board	*Representative*
ACI Worldwide	Doug Grote
American Bankers Association	Diane Poole
American Express Company	David Moore
Bank of America	Daniel Welch
Bank of New York Mellon	Arthur Sutton
Blackhawk Network	Anthony Redondo
Bloomberg LP	Corby Dear
Capital One	Marie LaQuerre
Citigroup, Inc.	Karla McKenna
CLS Bank	Ram Komarraju
Conexxus, Inc.	Gray Taylor
CUSIP Service Bureau	Gerard Faulkner
Delap LLP	Andrea Beatty
Delap LLP	Darlene Kargel
Deluxe Corporation	Angela Hendershott
Diebold Nixdorf	Bruce Chapa
Discover Financial Services	Michelle Zhang
Dover Fueling Solutions	Steven Bowles
Dover Fueling Solutions	Bradford Loewy
eCurrency	David Wen
Federal Reserve Bank	Mary Hughes
First Data Corporation	Lisa Curry
FIS	Stephen Gibson-Saxty
Fiserv	Dan Otten
FIX Protocol Ltd - FPL	Jim Northey
Futurex	Ryan Smith
Gilbarco	Bruce Welch
Harland Clarke	John McCleary
Hewlett Packard	Terence Spies
IBM Corporation	Todd Arnold
Independent Community Bankers of America	Cary Whaley
Ingenico	Rob Martin
ISARA Corporation	Alexander Truskovsky
ISITC	Lisa Iagatta
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Roy DeCicco
KPMG LLP	Mark Lundin
MagTek, Inc.	Mimi Hart
MasterCard Europe Sprl	Mark Kamers
NACHA The Electronic Payments Association	Priscilla Holland
National Security Agency	Paul Timmel
Nautilus Hyosung	Joe Militello
NCR Corporation	David Norris
Office of Financial Research, U.S. Treasury Department	Thomas Brown Jr.
PCI Security Standards Council	Troy Leach
RouteOne	Chris Irving
RouteOne	Jenna Wolfe

SWIFT/Pan Americas	Karin DeRidder
SWIFT/Pan Americas	Frank Vandriessche
Symcor Inc.	Debbi Fitzpatrick
TECSEC Incorporated	Ed Scheidt
The Clearing House	Sharon Jablon
U.S. Bank	John King
U.S. Commodity Futures Trading Commission (CFTC)	Robert Stowsky
USDA Food and Nutrition Service	Kathy Ottobre
Vantiv LLC	John Hall
VeriFone, Inc.	Dave Faoro
VISA	Kim Wagner
Wells Fargo Bank	Mark Schaffer

Under ASC X9, Inc. procedures, a study group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A study group exists only to study a specific item or technology determined by the X9 Board and is then disbanded after it generates a report. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the report. (Note: Per X9 policy, company names of non-member participants are listed only if, at the time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

At the time this Report was approved, the Distributed Ledger and Blockchain Technology study group had the following leaders and members:

Guy Berg, Chairperson
Angela Lawson, Editor

Organization Represented on the Study Group	***Representative***
American Express	Jonathan Gwynn
American Express	Jake Hershman
American Express	Kevin Walsh
Bank of America	Amanda Adams
Bank of America	Greg Nixon
Bank of America	Craig Palmer
Bloomberg LP	Inessa Collier
Bloomberg LP	Rich Robinson
Capital One	Bob Koshy
CLS Bank	Ram Komarraju
Discover Financial Services	Tyson Goings
Discover Financial Services	Cheryl Mish
Federal Reserve Bank	Rajeev Ranjan
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Ray Green
Federal Reserve Bank	Angela Lawson
Federal Reserve Bank	David Schwietz
Federal Reserve Bank	Heather Hultquist
Federal Reserve Bank	Mike Warner
Gilbarco	Bruce Welch
Hewlett Packard	Terence Spies
IBM Corporation	Todd Arnold
Intel	Jonathan Anderson
iStream Imaging/Bank of Kenney	Mike McGuire
iStream Imaging/Bank of Kenney	Mike McGuire
J.P. Morgan Chase	Elizabeth Aquino

J.P. Morgan Chase	Lance Harris
J.P. Morgan Chase	Luciane Sant'Anna
J.P. Morgan Chase	Darryl Scott
J.P. Morgan Chase	Leticia Lim
MasterCard Europe Sprl	Carl Jansson
MasterCard Europe Sprl	Michael Yu
National Institute of Standards and Technology (NIST)	Rene Peralta
National Security Agency	Laura Corcoran
RouteOne	Chris Irving
SafeNet Infotech Pvt. Ltd.	Amit Sinha
Silicon Prairie Online.	David Duccini
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Jay Wack
Thales UK Limited	Larry Hines
U.S. Department of the Treasury	Bill Nichols
U.S. Department of the Treasury	Jennifer Bond-Caswell
Upshot Advisors, LLC	Leland Englebardt
Verifone, Inc.	Joachim Vance
VISA	Ron Perez
VISA	Gyan Prakash
VISA	Kim Wagner
Wayne Fueling System	Bradford Loewy
Wayne Fueling System	Wes Mcafee
Wells Fargo Bank	Andy Garner
Wells Fargo Bank	Phillip Griffin
Wells Fargo Bank	Jeff Stapleton

ASC X9 Study Group Report

Distributed Ledger and Blockchain Technology Study Group

1 Scope and Purpose

1.1 Scope

Blockchain and distributed ledger technology as a whole can be applied in a wide number of industry segments ranging from property management and supply chain to underlying payment system settlement processing and digital currencies. While each of these areas could benefit from standards they also have very different market and regulatory requirements. Because of the high expectation for security, auditability and resiliency required in the heavily regulated financial services industry, the scope of this report is limited to blockchain-based distributed ledger technology applications specific to financial services. In addition, the Study Group determined that it was important to further delineate the distributed ledger technology trust model. (See Table 1) This report is limited to the "permissioned" trust mode, as the most likely to be adopted by financial services organizations.

Table 1

Blockchain Permission Models

		Who can make changes to the blockchain	Who can read information from the blockchain
In scope	Permissioned Public	Only authorized parties	Anyone
	Permissioned Private	Only authorized parties	Only authorized parties
Out of scope	Permissionless Public	Anyone	Anyone
	Permissionless Private	Anyone	Only authorized parties

Permissioned/permissionless refers to the ability to write to a blockchain. A permissioned blockchain restricts who can establish a node on and write to the ledger. In other words, the implementer has authority over which parties write to the blockchain, install smart contracts, and participate in the consensus process. Permissioned blockchains may allocate differential access. A permissionless blockchain allows any entity to write to the chain without restriction.

Private/public attributes refer to the ability to read information on the blockchain. On a private blockchain, the only parties who can read information are those who are authorized to do so by the owners of the blockchain, while public implementations may have unrestricted access for observers. Bitcoin, for example, utilizes a permissionless and public blockchain.

Current financial service applications would typically require permissioned private or permissioned public implementations. As the adoption and confidence in the technology grows it is possible that business cases will evolve for permissionless attributes to be acceptable even within financial services. However, for the purposes of this discussion, they will not be included in the scope of this work.

Due to the regulated nature of the financial market, certain requirements seem inevitable in a financial services context which may help provide guidance for standards. The limits of technology with respect to its role in financial services allowed the group, in part, to conclude that only a permissioned ledger will be workable at this stage (a fully "trustless" system appears incompatible with fully regulated solutions and the compliance and operational risks that financial institutions must manage.) Additionally, this consideration makes clear that those who build blockchain solutions for financial services would be well served to consider the applicability of established standards, particularly those that apply to acceptable security methods. For example:

- ANSI standards X9.69 and X9.73 provide attribute based access control, at the object level, enforced by cryptography and may be perfectly workable and a safe standard to integrate in a blockchain solution, rather than building a new solution out of whole cloth with the intent to apply it to a financial services use case.
- ANSI standard X9.84 provides biometric information management and security that can support multifactor user authentication.
- The trusted time stamps defined in X9.95 eliminate the need to coordinate time across multiple parties in a distributed ledger environment to provide simple, reliable notary services that can be audited. Stakeholders can rely on a single time source to determine the time of transactions globally, rather than attempting to coordinate time using multiple sources.
- X9.137 can provide tokenization management direction for confidentiality protection of blockchain data based on the cryptographic techniques defined in X9.119.

If considering the ISO 20022 framework with the use of blockchains, developers should consult ISO 20022 domains and message implementation guidelines for implementation details.

1.2 Purpose

This report provides an assessment of areas within the blockchain and distributed ledger architecture and system that would benefit from either establishing standards or complying with existing standards to assure a secure and effective blockchain implementation. To achieve this objective a common set of terms and definitions was necessary to effectively discuss the technology within the Study Group and with external experts. A glossary of those terms has been included in Annex A of the document. This document also provides an overview of the current state of blockchain and a reference architecture of a distributed ledger system in Annex B and C.

The Study Group limited its analysis to permissioned blockchains (as described above).This restriction is made on the grounds that regulated financial institutions require assurances with respect to the identity of those it serves and the ability to monitor, audit, and revise activity to meet legal and regulatory requirements.

Recognizing that distributed ledgers based on blockchain technology are a unique assembly of elements that have a broader use, the Study Group first considered the relevance of existing financial services standards that may be applied

directly to or modified for use in blockchain technology standards. Secondly, the group considered the need for the creation of new standards with particular relevance to blockchain. To effectively organize the analysis and corresponding report, categories for assessment were defined for the work. Within each category specific areas for a standards needs assessment were identified.

The categories are as follows:

1. *General Areas*
2. *Security – Cryptography and Key Management*
3. *Security of Transactions and Data Stored on or with the Chain*
4. *Access Control Requirements*
5. *Security requirements for platforms/components*
6. *Functions and Operation of the Blockchain*
7. *Smart Contracts (Chaincode)*

In acknowledgement of the balance between the use of standards to support new technologies and markets, and the desire to foster further innovations, the Study Group rated the areas in each category as *High*, *Medium* or *Low*, to indicate the importance of adherence to standards while developing blockchain implementations.

The Study Group further recommends that, wherever possible, existing standards be adopted for these areas when implementing blockchain technology.

Finally, the Study Group assessed the relative maturity of each area to determine if standards work could and should begin. Some areas have reached critical mass such that the need for standards work is clear, and the area is stable enough to begin discussions that will enable the safe and secure adoption of blockchain for industry participants. These areas are identified within the "Recommendation" portion of the assessment with a bold notation, **high priority**. The value of clear and common terminology for blockchain and distributed ledger technologies was immediately apparent. Work has already begun to standardize terminology through the X9 work group "Distributed Ledger Terminology Work Group." In addition, the other areas considered high priority and ready for standards development, as captured in detail on the following pages, are:

- Requirement to support migration to new algorithms over time,
- User enrollment process, vetting, etc.,
- Auditing—in the context of a blockchain within a distributed network,
- Node use lifecycle—lifecycle management of a blockchain within a distributed network,
- Long term data management of the chain,
- Logging—in the context of a blockchain within a distributed network.

2 Areas for Standards Work

This section presents the Study Group analysis of the value of standards work in blockchain. In order to create a methodology for assessing areas where standards may be needed, the Study Group began with broad categories of operational and security topics and examined each function individually. A rating of "High," "Medium," or "Low" was assigned to the importance and value of standards work. In this context, a "High" rating means considerable risk is present to the proper development of blockchain technology that may be remediated through the application of standards. A "Medium" rating means a moderate risk is present, and a "Low" would indicate little to no risk is present.

Our assessments and rating assignments do not necessarily define the specification of a single standard method for that function, but it may mean that work by standards bodies can streamline development and adoption of the technology by cataloging known, feasible, acceptable and (where necessary) interoperable methods that can be used. In some cases, a "High" priority on the value of standards may simply mean that control is necessary in order to avoid risks in developing and operating a blockchain.

2.1 General Areas

2.1.1 Definitions of blockchain terms: High

Throughout industry discussion of blockchain standards there is a common element: a call for common vocabulary. As blockchain innovation has developed in a myriad of independent efforts, the particular terms utilized have become similarly fractured. A first step toward shared efforts and potential interoperability is a clear and common vocabulary. Blockchain and distributed ledger discussions may use industry terms differently. For example, the word "consensus" has a particular relevance to blockchain applications. Nonetheless, there are different methods to achieve consensus and professionals may imbue distinct meanings to the term based on their familiarity with particular methods. A standardized terminology could enable more efficient cooperation and advancement of this technology by ensuring fewer miscommunications. In an effort to advance this work, the Study Group developed a list of common terms, some of which, as applicable to this report, are included as a glossary appendix in this document.[2]

Recommendation: Initiate a work group to develop a distributed ledger terminology standard. (In Progress.)

2.1.2 Legacy standard conflicts: Low

Because the application of blockchain technology is potentially far-reaching, with proposed solutions covering real estate title registration, securities issuance, cross-border payments, and many other use cases, there are likely a number of scenarios where standards already govern some aspect of the blockchain's function. For example, standards govern the acceptable cryptographic methods for securing card payment transactions. However, a blockchain solution may conflict with these existing standards in some cases, as when blockchain cryptography embraces more recent innovations that are not yet codified within other financial services uses.

Recommendation: The Study Group suggests that there may not be a way to standardize an approach to incorporating existing standards or standards conflicts. On a case-by-case basis, developers may need to assess how to resolve these conflicts in order to preserve innovation. No standards work is recommended at this time.

[2] Additional terms were developed as part of the work of this Study Group. Given the scope of work of the DLT Terminology Work Group, the full draft glossary was provided to the work group for continued discussion and development and therefore not included in this report.

3 Security – Cryptography and Key Management

3.1 Identifiers indicating what algorithms and key lengths are used in the chain: High

Standardized identifiers are essential for clear, concise, and consistent communication of an implementation's cryptographic characteristics. The security strength is determined by the algorithms and key length employed. Miscommunication of cryptographic implementation details can lead to weakening of security of the system.

Recommendation: It is highly recommended that existing standardized identifiers be adopted.[3]

3.2 Requirement to support migration to new algorithms over time: High

Blockchain cryptography is subject to change over time. Cryptography applied to a given block must be properly identified. Otherwise, relying parties may lose their ability to gain assurance in the integrity and authenticity of stored content, and risk loss of access to any encrypted or tokenized data. The draft X9.125 standard proposes to addresses these issues with a Cryptographic Algorithm Status Transition (CAST) block. Other techniques should also be explored for possible standardization.

There are many reasons that cryptography may change. Key lengths tend to grow as computers become faster. Successful attacks and flaws discovered by researchers can reduce algorithm strength or increase their vulnerability to compromise. New algorithms may be created that feature superior characteristics of processing speed, and memory or storage requirements.

Changes in organizational security policies, government export restrictions, or within the legal or regulatory jurisdictions in which cryptography is deployed can impact suitability and necessitate changes in cryptographic solutions. All of these aspects can drive the need to replace cryptography in current use and to migrate to others.

Recommendation: Standardization efforts that support cryptographic algorithm agility should be given **high priority** in the near term. Standards work should begin in the 2018-2019 time frame.

3.3 Key Management – General (key creation, derivation, distribution, storage, etc.): High

The proper management of cryptographic keys is essential to their effective use and the overall security of the applications/systems.[4] If a key is compromised the applications/systems that use that key are effectively vulnerable to compromise. Secure key management systems, procedures and policy are essential to protecting cryptographic keys that are used for cryptographic operations in applications. A key management system does not use the keys but rather managers the security, creation, derivation, distribution, storage, and other administrative security audit functions. Blockchain systems incorporate a variety of asymmetric, symmetric and hashing keys that need to be effectively secured and managed to protect the blockchain system from compromise. Following key management standards in this area is of high importance because it is both a critical and complex element of the technology.

Recommendation: Review the Key management standards to ensure that the current body of work covers cryptographic innovations and is incorporated in blockchain systems. For example, do existing key management standards sufficiently cover elliptic-curve key management requirements which may be incorporated in certain

[3] See e.g. RFC 5758, "Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA", Internet Engineering Task Force, January 2010. https://tools.ietf.org/html/rfc5758.

[4] Elaine Barker, National Institute of Standards and Technology, "Recommendation for Key Management Part 1: General", SP 800-57 Pt. 1 Rev. 4 (January 2016). http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

blockchain systems? It is important to review and update X9 standards to support the use of contemporary cryptographic algorithms and provide industry confidence in their application by blockchain system designers.

3.4 Key Management – Rotation, destruction, and replacement (change when required due to key compromise, key crypto period expiration, etc.): High

Despite the pains taken to avoid compromise with proper general key management procedures, a system may nonetheless be obligated to use exception processes when a user loses a key, a key expires, or is otherwise compromised. Standardization of key management for rotation, destruction, and replacement is a high level area because of the importance in limiting risk exposure.[5] Theft of secret or private keys is a risk which can be mitigated by limiting the key's validity period and amount of use.[6] Some blockchains today do not have any designated means of replacing a compromised key, resulting in end user losses. This level of vulnerability is unacceptable in a financial services environment.

Recommendation: Blockchains that use financial services data should consider adherence to existing X9 standards for security in handling financial data.

3.5 Cryptographic algorithms and key lengths that can be used: Medium

Standardization of cryptographic algorithms and key lengths for Blockchain application is a medium-level area because the choices will ultimately depend on the level of protection required for a particular use-case. Keys are selected to be resistant to some predetermined level of attack. The trade-off between longer key size and computational costs must be analyzed within the context of the application. There are some crypto innovations, including elliptic-curve, that do not yet have well established standards but are generally accepted to meet rigorous security criteria to achieve the target level security required for financial markets.

Recommendation: Blockchains must use X9 approved cryptographic algorithms and key lengths. No standards work needed at this time. Existing cryptographic algorithm standards can be relied upon to make this type of determination.[7] Future developments in quantum computing may impact best practices.[8] Cryptographic agility standards for Blockchain will allow for changes in algorithms as needed.

4 Security of Transactions and Data Stored on or with the Chain

To assess the need for standards related to transaction and data storage security it is important to clearly understand what aspects of security are integral to a blockchain system and for what aspects of security a blockchain system relies upon other systems and procedures in the surrounding environment.

Blockchain assures integrity by delivering the promise of "immutability;" which in this context means the assurance of an indelible, permanent record of any element added to the blockchain. However, in reality, the core functionality of a blockchain does not enable immutability per se but rather the ability to detect changes once a transaction is posted to

---

[5] Accredited Standards Committee X9, Incorporated Financial Industry Standards, "Public Key Infrastructure (PKI) —Part 4: Asymmetric Key Management —for the Financial Services Industry", ANSI X9.79-2013. February 5, 2013.

[6] See e.g. David Balaban, "Five Biggest Bitcoin Exchange Hacks", September 19, 2016. http://cryptorials.io/5-biggest-bitcoin-exchange-hacks/.

[7] See e.g. "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve

Digital Signature Algorithm (ECDSA)", ANSI X9.62; Federal Information Processing Standard (FIPS) 140, 180, 186, 198 provide details of cryptographic algorithm implementations. http://csrc.nist.gov/publications/PubsFIPS.html.

[8] Dustin Moody, National Institute of Standards and Technology, "Post-Quantum Cryptography: NIST's Plan for the Future", 2016. http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/pqcrypto-2016-presentation.pdf.

the distributed ledger. Any given copy of the ledger, like any digitally stored data, can be amended at any time. A consensus process requires those changes to be reconciled to distributed copies of the blockchain. The cryptographic hash on the data is the technology that enables the detection of changes. In this way, the permanence of any data in the blockchain is dependent on strong cryptographic hashing processes and well-functioning consensus processes. In addition, blockchain systems typically do not encrypt data on the chain so do not provide confidentiality, which means that sensitive data stored on the chain can be viewed and stolen. This means that standard system and data security practices need to be applied to blockchain systems to achieve data security. This key point was considered when assessing the need for standards application in the following areas.

4.1 Parts of the blockchain to be protected: Low

Financial services typically deal with distinct types of data of varying sensitivity, from statutorily protected information to public records. According to the risk requirements, these data elements receive varying protections in the corresponding information systems, and are often stored under distinct systems. Blockchain architectures may collect a variety of data and objects within the overall solution. Information on blockchains may include identity assertions, content of multiple types, support information, smart contracts actions/directives, time stamps, validations and regulations etc., (see reference architecture). As such, the framework of the overall system should be able to address all objects as well as address the secure, confidential, differential access to any and all objects within a given transaction.

Recommendation: No standards work is recommended at this time.

4.2 Confidentiality requirements: High

When assessing the need for standards related to confidentiality, we considered the extent to which blockchain technology inherently provides, or does not provide, protection of confidential or sensitive data that could be harmful or damaging if exposed to unauthorized individuals. Whether in a permissioned or permissionless blockchain, data integrity is provided through hashing but there is no standard mechanism inherent within blockchain to deliver confidentiality.

Recommendation: While blockchain systems do not inherently provide confidentiality for data on the chain, they do not introduce any new requirements or barriers for achieving data confidentiality that is not addressed within X9 and other standards bodies. At this time there is no need for additional standards work to address confidentiality requirements within the financial services industry segment for blockchain systems.

4.3 Data integrity requirements for data within the chain: High

Data integrity involves the assurance that information can be acted upon and will continue to offer a consistent message over time. The foundation of the blockchain technology is the belief the data within the structure cannot be altered without detection after being written. This is achieved by securing data integrity with a hash (typically using a Merkle tree). There are multiple mechanisms to achieve this assurance. The use of cryptography, hashing functions, and other mathematical processes are available in security standards. For example, using existing ANSI standards (e.g., X9.69/9.73) provides attribute-based access control to any digital object, maintaining confidentiality, data integrity, authentication, and differential access control, persistently, over the entire life-cycle of the transaction data life. Blockchain implementations should follow the guidelines provided by these standards.

Recommendation: At this time, there are many perceived needs for additional work in standards for data integrity requirements for data within the chain to support blockchain adoption and development. Though standards for hash algorithms exist and should be used.

4.4 Security requirements for data at rest (if not covered by categories above): High

Data at rest refers to the information that is stored over time in a particular application. Blockchains may hold a number of data objects in the course of creating a reference ledger. The process of providing persistent protection and access

control to all of the data objects in a given application can be accomplished by the use of existing ANSI standards (e.g., X9.69 and X9.73 which enable the creation of self-protecting data objects that are data label aware, with services based on that awareness, enforced by cryptography). It remains a high priority to apply such standards to the maintenance of data within blockchain applications.

Recommendation: There is no need for additional work in standards for security requirements for data at rest to support blockchain adoption and development as they already exist.

4.5 Access control and process management: Medium

In addition to processes that protect stored data, an application must also develop policies for compliance, certification, and audit that ensure all users operate in a manner that maintains the integrity of the system. Financial services participants will and should have concerns about the environment in which their blockchains operate. A certain level of trust is required in order to operate in a blockchain environment with concerns about regulatory requirements, privacy, etc. (especially since blockchain applications may be borderless and operate internationally). While potentially out of scope for X9, these are areas that may be considered to facilitate documented policies to assess compliance with the agreed operation of the ledger.

Recommendation: Blockchain users should use clear and auditable procedures to protect access control and process management of a blockchain application. No standards work is recommended at this time.

5 Access Control Requirements

5.1 User enrollment process, vetting, etc.: High

Enrollment is the process of effectively authenticating a user in order to grant them access to a secure system. As the security of a system increases, so do the requirements for application of a rigid and robust identity authentication vetting process. A permissioned blockchain is a secure environment and users at all levels of access permissions must be enrolled in the system before conducting activity on it. Lack of appropriate authentication procedures in the enrollment process presents one of the greater points of vulnerability to blockchain systems. Security standards applied to enrollment processes help reduce the risk of internal attacks.

Recommendation: Standardization work on the enrollment processes for blockchain should be a **high priority** for developing secure blockchain applications in the financial services environment.

5.2 Predefined user levels (e.g., user, auditor, administrator, etc.): High

Predefined user levels allow a systematic means of administering differential access. It is a standard information security practice for some users to have read only access while others have read/write access to certain subsets of information within the application. Typically, this is accomplished by defining certain roles for distinct user groups and administered by assigning roles to users for access control. Access control is complex and difficult to configure. By having predefined access control settings for common user levels, the likelihood that blockchain administrators will make mistakes in access control definitions is greatly reduced. Reduced administration complexity can improve the robustness and security of the blockchains. Standardization of blockchain user levels can establish a model for security as well as create clarity about the roles individuals can expect to play as they participate in blockchains.

Recommendation: Standardization work in this area may accelerate interoperability and adoption of blockchain technology and may reference the NIST model established in special publications on role-based access control and attribute based access control (RBAC and ABAC).

5.3 Authorization (to perform transactions and other operations on the blockchain): Low

An authorization system determines if a requested operation is permitted. While it is a fundamental piece of security, there are numerous valid methods of authorizing an operation. Authorization is an extension of the access control processes in a permissioned blockchain.

Recommendation: While it is important for any given blockchain application to define its requirements for an authorization system, it is not important to standardize the way in which that authorization system works across different blockchains. Standardization would be of limited benefit for this issue. No standards work is recommended at this time.

6 Requirements for Using a Secure Cryptographic Device (SCD)

6.1 At the Server: High

Existing standards (ISO 13491/ X9.97) define secure cryptographic devices and delineate distinct physical and logical characteristics for cryptographic processes. At the server level, an SCD may be involved in cryptographic functions like:

- authentication of incoming communications to ensure validation,
- hashing of data on the blockchain,
- possibly encryption/decryption of data coming through communications channels,
- encryption and decryption of data on the blockchain itself,
- protection of communications channels (TLS session between node and client).

Depending on the architecture of the system, these functions may be spread across one or more servers and some functions may not be implicated.

The security (use of SCDs) will tend to be related to the requirements of the data that is used on the blockchain. For example, standards may govern the handling and protection of account information (X9.119). Depending on the data used, financial service blockchains need to adhere to the standards applicable to the protection of its data, as well as the policies of the organization that owns the data.

Recommendation: It's important to follow established standards where applicable to data considered for blockchain use. Standardization work may be required to review broader blockchain use cases and determine whether there are gaps between the way that blockchains handle data and the standards for those data types under conventional processes. The need for data protection for SCD is not blockchain driven, it is business application driven. No standards work is needed at this time, though recommend reassessment in 2019.

6.2 At the Client: High

A secure client may be necessary to protect a private key (or other credentials) to prevent impersonation. There appear to be relatively few applications of client-side SCD at present. In the future a Secure Execution Environment on a mobile device may operate as a client side SCD. Depending on the data that is being handled, there may be a need to ensure that data cannot be inadvertently revealed or stolen.

Recommendation: Based on specific use case, where user credentials in the form of private key, PIN, biometric or other data needs to be protected and if a secure cryptographic device is required, manufacturing, deployment and operations standards for an SCD must be applied.

6.3 Security of time source to timestamping: High

Timestamping is a function that assures the proper sequence of changes in a system. Secure timestamps are fundamental to the security of the current state of a system, since an alteration in the order of events can affect the

present outcome or the validity of updates. Many applications using blockchain will have critical requirements on the times of events and the relative times between events. A secure, consistent, auditable source of time for these events is very important. Notary services based on X9.95 will support implementations that can meet such requirements.

Recommendation: Blockchains that rely on a timestamp function should apply relevant standards to ensure the security of the timestamp. No standards work needed at this time.

7 Security requirements for platforms/components

7.1 Use of the server to run other applications: High - Proportional to risk

Higher security is required for some applications more than for others. In some cases, the risk of using the server for multiple different applications will not be acceptable, because of the possibility of leakage between applications or attacks by a malicious application. The most sensitive blockchain applications have a strong requirement for an isolated execution environment. Controls such as virtual machines or separate containers are often applied to any application with sensitive data.

Recommendation: Depending on the security requirements of the application the blockchain is supporting, consideration of appropriate controls will be critical. The application is the driving force. This is not unique to blockchain. No standards work needed at this time.

8 Functions and Operation of the Blockchain

8.1 Interface APIs/Protocols used to submit requests: Low

API interfaces and protocols allow interaction with the data and functions managed within an application. Users can request blockchain services over a network using APIs and protocols. On one hand, the development of standard interfaces is fertile ground for standards. For outward facing communications, there may be standards that are well suited (e.g., ISO 20022 can serve as a basis) to blockchains. On the other hand, the communications that blockchain applications may need to receive are still under development and innovation. At this stage of technology development, specifying what types of APIs a blockchain should receive may be limiting.

Recommendation: No standards work needed at this time.

8.2 Interoperability: Low

Interoperability can be a key consideration for applications that form part of an integrated system. Blockchain applications to date are almost exclusively customized and purpose built.

Recommendation: While there may be groups working on feasible means for accomplishing specific functions across distinct blockchains, overall standards work on this area can be desirable in some cases, but is a low near-term priority.

8.3 Structure of data stored: Low

Specific data structures allow easy exchange and readability of data from one system to another. Communication to a blockchain will occur through an API or interface with specific requirements for the format of that file. The underlying structure of the data may not be important to users. As long as the elements of sufficient communication are stored within a blockchain, the format in which they are stored is unimportant. When distributed ledgers become systems of record, it may be necessary to specify how to structure the data therein for easy reference. At present, blockchains are still proving purpose built, permissioned uses.

Recommendation: The merit of such standards is not yet clear and remains low priority.

8.4 Consensus methods: Low

While a number of consensus methods have been devised and proven, there are still emerging methods in this space. Innovation continues on this front, devising consensus processes and methods to suit the specific tradeoffs desired for a given application.

Recommendation: Standardization might serve to catalogue a number of workable alternatives, but the priority to do so remains low.

8.5 Auditing: High

Auditing can refer to both the financial accounting and compliance audits as well as forensic investigations and regulatory review. The potential of blockchains in financial services clearly creates a need to support audit functions that can comply with requirements of financial services and meet the general needs of the stakeholders for reliable auditability. Access control can enable differential access for necessary audit functions while appropriately restricting access to data on the blockchain. Development of standards around audit functions would allow for more rapid adoption and elaboration of the technology without requiring each application to solve this issue independently. In particular, standardized event journal content and formats may be beneficial, and journal security based on X9 approved security techniques can ensure the data integrity and origin authenticity of this information. Techniques described in X9.125 could also provide a blockchain-based framework for the secure collection of compliance data needed to support auditing, risk management, and governance of distributed systems.

Recommendation: To address regulatory requirements, a workgroup should be initiated as a **high priority.**

8.6 Node validation and recognition: High

Computer systems in a variety of contexts have the need to validate each other as authorized for interaction. In a distributed ledger, each node must recognize the validity of work conducted by peers to form a consensus around the current version of the blockchain ledger. This can typically be achieved by enrolling nodes and using digital certificates. While there may not be a single specific method to allow nodes to recognize the validity of peers, it is crucial that distributed ledgers use some acceptable method to do so.

Recommendation: The onboarding of nodes in a closed system, where the addition of a node is controlled, can apply existing mutual authentication standards. No standards work is recommended at this time.

8.7 Node life cycle: High

Over the course of its life, a distributed ledger will need to onboard and sunset a number of peer nodes as institutions join and leave the network. The node of a blockchain is an entry point into a secure and highly trusted environment and can be a vulnerable point of attack if proper node lifecycle management practices are not followed. In addition, the definition of standards to provide guidance in the techniques for handling node onboarding and sunset would contribute to consistent security practices and common management processes across blockchain applications

Recommendation: Lifecycles standards have been established for a variety of applications and devices serving the financial industry including mobile devices, mobile wallet applications, ICC chips and their applications. In each of these cases a standard exists that facilitates common practices for management procedures, policies and applications. Development of a similar lifecycle standard for nodes on a blockchain could enable common node management practices while supporting consistent security across blockchain platform providers. Standards work in this area is a **high priority** and should be initiated in 2018-2019.

8.8 Long term Data Management of the Chain: High

A strict definition of a blockchain suggests that removing data violates one of the core attributes. There may be cases where some data on a blockchain may need to be removed from the active chain and placed in an acceptable archival format and medium for one business reason or another. For example, there could be a smart contract with an application rule set that may require removal of data after a certain period of time. This topic is highly controversial given the fact that a core principle of blockchain technology is the completeness of the history of the data on the chain. Nevertheless, it has been suggested by some that it may be necessary to remove data on a chain.

Recommendation: The concept of removing data a blockchain has great significance and impact on the base integrity of the chain. For this reason, the industry should address this subject with care through standards development and guidance. A workgroup should be initiated to address this **high priority** issue.

8.9 Correcting Errors in Transactions: High

True immutability – that is, a ledger that cannot be amended under any circumstances – means that errors may not be corrected by deleting data from the ledger. In financial use cases, however, there may be a true need to correct a transaction. Standards work within the blockchain community may help resolve how proper records can be maintained while balancing the feature of purported immutability. Industry work will need to resolve this tension between a much touted feature that enables trust in the permanence of the record and the reality of the need to accommodate changes and error correction in that transaction.

Recommendation: Transaction error corrections should follow standard financial industry practices where offsetting transactions are used to correct erroneous transactions. No standards work is recommended at this time.

8.10 Sidechains/Subchains: Low

There are widely different interpretation of the structure, security and operational roles of sub and side chains. The definition of a sidechain/subchain is still subject to debate. The following is one definition but other definitions are possible: *A side/sub subchain is a logically separate chain that forms part of a blockchain. Each subchain may be owned by a different entity and may be accessible to a different set of users.* This is a new concept introduced by blockchain technology that has not been addressed by standards in the past. That in itself does not necessarily mean that additional standards work is required.

Recommendation: This is an important topic for standardization after further time for maturation of the function.

8.11 Logging: High

Logging is defined as a trace of any system activity of record performed, viewed and changed by whom and at what time. In blockchains the history of transaction is maintained on the chain itself, however, it does not include other node activity that is not directly related to the chain transaction. It is feasible for a blockchain to maintain the necessary elements of a log within the chain itself, but it is also likely that blockchain systems will have distinct logging requirements for off-chain activity to adequately maintain a history of all user activity on a node. Should logs be node specific or should a blockchain system maintain a single log for all node user activity? These requirements may vary based on business requirements. Standard may make an important contribution by providing guidance on the type of logging required for different uses of blockchain in the financial services industry.

Recommendation: Logging plays a significant role for problem troubleshooting, error resolution and security audit controls. Standards development in this area would provide valuable guidance to achieve proper and consistent logs to support security controls and system auditors. A workgroup should be initiated to begin addressing this **high priority** area.

9 Smart Contracts

9.1 Functions permitted: Medium

Smart contracts could conceivably be written to execute functions that have great consequences to a chain. What level of restrictions, if any, should be placed on functions performed by smart contracts? Standards that control what smart contracts are permitted to do on a blockchain could provide necessary industry guidance to reduce risk of functions that could negatively impact the integrity or security of the chain. For example, smart contracts should alter neither access control data for users, nor access or change functions within the operating system. They should not have the ability to modify system logs of any kind.

Recommendation: Standard should be developed to provide industry requirements and guidance to avoid consequences of unrestricted smart contract functions that could negatively impact a chain's data integrity, security and platform stability. Recommend consideration for 2018 work due to the rapid pace of development in some industries.

9.2 Interaction with external applications: High

Smart contracts will inevitably interact with applications outside of the blockchain itself. Whether this is by referencing an "oracle" to secure data about some event in the world that effects the execution of code or by creating output to be acted upon by an external application, this code will need to find a home in blockchain receptive applications. Currently there are no industry guidelines for minimizing the risk of introducing security vulnerabilities when interfacing to external applications. In addition, blockchains are designed with the requirement to stay in synch with all nodes on the chain. However, external applications on separate nodes that interact with a chain are not necessarily designed to stay in synch. Currently there are no industry standards for addressing the methodologies for assuring that each node sees consistent data from external applications and need to ensure that nodes do not duplicate actions on an external application.

Recommendation: Standards should be developed for smart contract interactions with external applications to provide guidance to protect integrity, security and stability. Though this is important work, the technology needs time for maturation before standards work can begin. Recommend reassessing in 2019.

9.3 Programming languages: Low

Blockchains could conceivably host code written in a number of languages. Innovation is still prevalent in adapting or creating languages used for creating smart contracts.

Recommendation: No standards work needed at this time.

9.4 Security of code installation: High

In a blockchain system, it is of paramount importance that smart contract code is correct and is identical on all nodes. If an attacker has the ability to install malicious or incorrect smart contract code, he or she can alter the behavior of the smart contracts and cause legal, financial, and other consequences. When smart contract code is installed on the system, there must be assurances that the code is from the correct trusted provider and that it has not been modified. Furthermore, there must be controls to ensure it can only be installed by authorized personnel. Standards can provide guidance in each of these areas.

Recommendation: Security of code installation is a high priority security issue for platforms that permit the use of smart contracts. Standards should be developed to address this point of vulnerability. Though this is important work, the technology needs time for maturation before standards work can begin. Recommend reassessing in 2019.

9.5 Security of executing a smart contract: High

A smart contract may be programed to execute and complete a transaction only under certain conditions, for example, in an escrow transaction. A smart contract also can be executed from an API function. The execution of a smart contract when it is not appropriate could have disastrous effects. Methods currently exist to authorize software functions and similar techniques should be used for the execution of smart contracts.

Recommendation: The full impact of smart contracts and associated execution security is not well understood at this point in time. While there are existing methods for securing the execution of software, new cases may arise that are unique to smart contracts. Existing methods may be considered sufficient for current blockchain implementations; however, it should be revisited after the technology has more time to develop. Though this is important work, the technology needs time for maturation before standards work can begin. Recommend reassessing in 2019.

10 Conclusions & Recommendations

The state of blockchain and distributed ledger technology remains in flux at the close of 2017. While the applicability of standards for blockchain applications in the financial services sector is clear in many cases, much remains to be seen as the technology matures and use cases develop in production environments. To that end, the Study Group recommends that operators use caution during the development phase and should seek to apply current, existing standards. The industry, meanwhile, should approach the application of standards as a whole in three stages.

First, assess the application of existing standards. In many cases, the Study Group found that blockchain did not represent any new risks or challenges not already addressed by current standards. For example, defining standards for the use of a server to run other applications or for using a secure cryptographic device is not unique to blockchain. Though standards apply, there is no blockchain-specific standards work needed at this time.

Second, where blockchain-specific needs exist (or evolve over time) seek appropriate incremental work through maintenance agencies. For example, cryptographic algorithm standards exist today, but advances in blockchain technology and adoption may speed the need for additional agility in updating standards in this area. Much of this depends on the maturity of the technology and how it develops. In some cases incremental improvements will match the need. In other situations, the industry may discover a new standard is needed once more is known.

Finally, some areas have reached critical mass such that the need for standards work is clear, and the area is stable enough to begin discussions that will enable the safe and secure adoption of blockchain for industry participants. In cases such as those the Study Group deemed “High Priority,” including:

- Requirement to support migration to new algorithms over time,
- User enrollment process, vetting, etc.,
- Auditing—in the context of a blockchain within a distributed network,
- Node use lifecycle—lifecycle management of a blockchain within a distributed network,
- Long term data management of the chain,
- Logging—in the context of a blockchain within a distributed network,

work should begin in the relatively near term (2018-2019).

As we’ve seen with the inception of the X9 Distributed Ledger Terminology Work Group, interest across the industry to participate in helping to define and support this emerging technology is great. Encouraging those with both the expertise and the will to shepherd blockchain technology towards its fruitful and efficient adoption can only improve the experience of industry participants looking to capitalize on the benefits of this and other innovations over time.

Annex A

Glossary of Terms

The Study Group assembled this glossary of terms largely through referencing existing work and compiling terms from ANSI, the American Bar Association, Blockchain Technology Glossary, Blockchainhub Berline, CoinDesk, IBM Glossary for Hyperledger Blockchain, and PAXOS the Repository.

Asymmetric Cryptographic Algorithm	Cryptographic algorithm that has two related keys, a public key and a private key; the two keys have the property that, given the public key, it is computationally infeasible to derive the private key
Auditability	In blockchain, the compliance with regulations and ability to keep an accurate record of all transactions, processes, and actions.
Authentication	The process of validating the identity of a user or server.
Authorization	In computer security, the right granted to a user supporting access to digital objects: physical, logical, functional or content.
Block (on the blockchain)	Data is permanently recorded in a blockchain network through files called blocks. A block is a record of some or all of the most recent transactions that have not yet been recorded in any prior blocks. New blocks are added to the end of the record (known as the blockchain), and are tamper resistant once written. Each block memorializes what took place when it was created. Each block contains a record of some or all recent transactions, and a reference to the block that came immediately before it. Because each block contains a reference to the prior block, the collection of all blocks in existence can be said to form a chain. However, it's possible for the chain to have temporary splits – for example, if two nodes arrive at two different valid solutions for the same block at the same time, unbeknownst to one another. A peer-to-peer network is designed to resolve these splits within a short period of time, so that only one branch of the chain survives.
Blockchain	A blockchain is a type of distributed ledger, cannot be changed without detection, digitally recorded data in packages called blocks. Each block is then 'chained' to the next block, using a cryptographic hash. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions. This can maintain an ever-expanding list of data, each referring to previous items on the list, creating an incorruptible digital record. Blockchain was initially introduced as Bitcoin's underlying technology. Unlike their initial application on the Bitcoin network, blockchains do not have to be tied to bitcoins or any cryptocurrency and may be private and permissioned. This is the preferred usage of blockchain technology in the financial services industry, often referred to as financial blockchains or distributed ledgers.
Business Rule	A representation of how business policies or practices apply to a business activity.

Certificate	A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.
Certificate Digital Certificate	public key and identity of an entity, together with some other information, that is rendered unforgeable by signing the certificate with the private key of the Certification Authority that issued the certificate.
Certificate Authority CA)	Entity trusted by one or more other entities to create and assign certificates.
Certificate Revocation List (CRL)	A list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted. CRLs are a type of blacklist and are used by various endpoints, including Web browsers, to verify whether a certificate is valid and trustworthy.
Chain Validator	A blockchain role that owns a stake of a chain network. Each chain validator can decide whether a transaction is valid and can interrogate all transactions sent to their chain.
Chaincode	Executable code that is deployed on a blockchain network, where it is executed and validated by chain validators together during the consensus process. Developers can use chaincodes to interact with a network's shared ledger, develop business contracts, asset definitions, and collectively-managed decentralized applications.
Clearing and Settlement	Process through which assets are exchanged for payment. This process takes place after a trade is executed and is an integral part of the post-trade cycle.
Client	A software program a user executes on a desktop, laptop or a mobile device to launch an application.
Confidentiality	In a blockchain, the ability to render the transaction content inaccessible to anyone other than the stakeholders of the transaction.
Confirmation	A confirmation means that the blockchain transaction has been verified by the network. This happens through a consensus process specific to a given blockchain. Once a transaction is *confirmed*, it cannot readily be reversed or double spent.
Consensus	The process of participants in a blockchain agreeing to a transaction and validating it through the peer network. Consensus ensures that shared ledgers are exact copies, and lowers the risk of fraudulent transactions since tampering would have to occur across many places at the exact same time.
Cryptocurrency	A form of digital currency based on mathematics, where cryptographic techniques are used to regulate the generation of units of currency and verify the transfer of funds. Furthermore, cryptocurrencies operate independently of a central bank.

Cryptographic Hash Function (Hash)	(Mathematical) Function that maps values from a large (possibly very large) domain into a smaller range and satisfies the following properties: 1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output; 2. (Collision Free) It is computationally infeasible to find any two distinct inputs that map to the same output.
Cryptographic Key (Key)	Parameter that determines, possibly with other parameters, the operation of a cryptographic function such as: (a) the transformation from plaintext to ciphertext and vice versa; (b) the synchronized generation of keying material; (c) electronic signature computation or validation.
Cryptography	Discipline that embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof
Digital Signature	A cryptographic transformation of data which, when associated with a data unit, provides the services of: (a) Origin authentication (b) Data integrity, and (c) Signer non-repudiation
Distributed Ledger	Distributed ledgers are a type of database that is spread across multiple sites, countries or institutions. Records are stored one after the other in a continuous ledger. Distributed ledger data can be either "permissioned" or "permissionless" to control who can view it.
Distributed Ledger Technology (DLT)	Technology that allows any participant in the network to see the records of ledgers for all the participants in the network.
ECDSA (Elliptic Curve Digital Signature Algorithm)	The Elliptic Curve Digital Signature Algorithm is the lightweight cryptographic algorithm used to sign transactions in the Bitcoin protocol.
Endorsement	A collection of digital signatures from endorsing peers that establish that a transaction satisfies an endorsement policy.
Endorsement Policy	A condition on a transaction.
Endorser	See endorsing peer.
Endorsing Peer	A node that endorses a transaction before it is committed.
Escrow	The act of holding funds or assets in a third-party account to protect them during an asynchronous transaction. If Bob wants to send money to Alice in exchange for a file, but they cannot conduct the exchange in person, then how can they trust each other to send the money and file to each other at the same time? Instead, Bob sends the money to Eve, a trusted party who holds the funds until Bob confirms that he has received the file from Alice. She then sends Alice the

	money.
Exchange	A central resource for exchanging different forms of money and other assets. Bitcoin exchanges are typically used to exchange the cryptocurrency for other (typically fiat) currencies.
Fiat currency	Any money declared by a government to be to be valid for meeting a financial obligation, like USD or EUR.
Financial Blockchains	Recent applications of blockchain technology in financial services involve the use of private, permissioned distributed ledgers that can help expedite the clearing and settlement of assets and deliver enhanced record-keeping.
Hash (see Cryptographic Hash Function)	
Hyperledger Fabric	The implementation of the Linux Hyperledger project. See also Linux Hyperledger project.
Identity	The collection of specifications, rules and legal obligations necessary to establish uniqueness of participants in any transaction.
Key (see Cryptographic Key)	Parameter that determines, possibly with other parameters, the operation of a cryptographic function such as: (a) the transformation from plaintext to ciphertext and vice versa; (b) the synchronized generation of keying material; (c) digital signature computation or validation
Key Management	Generation, storage, secure distribution and application of keying material in accordance with a security policy.
Key Pair	Public key and its corresponding private key used in public key cryptography.
Ledger	A system of record of transactions.
Linux Hyperledger project	An open source, collaborative effort to advance blockchain technology by identifying and addressing important features for a cross-industry open standard for distributed ledgers that can transform the way business transactions are conducted globally. Hyperledger serves as the foundation code for the IBM Blockchain products, services, and solutions. See also Hyperledger fabric.
Merkle Tree	A Merkle tree is a concept that has a piece of data that is linking to another. This is often achieved by linking with a cryptographic hash. The content itself can be used to determine the hash. By using the cryptographic hashing, existing content can be made immutable because if you change anything in the data invalidates all subsequent references until the entire tree is re-worked.

Node (Full Node)	Any computer that connects to the blockchain network is called a node. Nodes may enforce the rules of the blockchain and form the backbone of the network.
Object	That which is to be encrypted…any named digital string: logical; functional; content.
Object Key	Key used to encrypt and decrypt an object.
Oracles	Smart contracts on the blockchain cannot access the outside network on their own; therefore oracles sit between a smart contract and the external world, providing the data needed by the smart contract to prove performance, while sending its commands to external systems.
Participant	An actor who can access the ledger: read records or add records to.
Peer	An actor that shares responsibility for maintaining the identity and integrity of the ledger.
Peer-to-Peer	Pertaining to a form of distributed processing, in which the front-end and back-end of a conversation switch control between themselves. It is communication between equals.
Permissioned Ledger	A blockchain network where each node is required to be a member of the network, and each node has access to only the transactions that its permissions allow.
Permissionless Distributed Ledger	Participants in this distributed ledger network may remain completely anonymous. Although most permissionless ledgers are public ledgers, they could also be private.
Privacy	In blockchain, the concealment of chain transactor identities on a network. Members of a network may examine the transactions, but the transactions can't be linked to the transactor without special privilege.
Private Blockchains	A fully private blockchain is a blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Likely applications include database management, auditing, etc. internal to a single company, and so public readability may not be necessary in many cases at all, though in other cases public auditability is desired.
Private Key	In an asymmetric (public) key cryptosystem, the key of an entity's key pair that is known only by that entity NOTE A private key may be used to compute the corresponding public key, to make a digital signature that may be verified by the corresponding public key, to decrypt data encrypted by the corresponding public key; or together with other information to compute a piece of common shared secret information.
Public Key	That key of an entity's key pair that may be publicly known in an asymmetric (public) key cryptosystem. NOTE A public key may be used to verify a digital signature that is signed by the corresponding private key, to encrypt data that may be decrypted by the corresponding private key, or by other parties to compute shared information.

Sidechains	Blockchains that are interoperable with another blockchain. Sidechains allow blockchains to perform functions that are linked or pegged to another record, without congesting the original blockchain. For example, cryptocurrency sidechains can be backed by bitcoins, via bitcoin contracts that link to the bitcoin blockchain, which in turn could iterate to implement experimental sidechain features once they have been tried and tested
Signature	A digital digest produced by hashing keys or other components together to prove that a transaction came from a particular address.
Smart Contract	A set of business terms that are embedded into a blockchain and executed with transactions. A smart contract can also include a digital representation of a set of business rules and defines conditions under which transfers occur.
Subchain	A subchain is a linked but logically separate chain within a blockchain.
Supply Chain	A value chain that supports procurement and sourcing of goods.
Transaction	A request by a transactor to the blockchain to execute a function on the ledger.
Transaction Block	A collection of transactions on the bitcoin network, gathered into a block that can then be hashed and added to the blockchain.
Permissionless Ledgers	Permissionless ledgers such as Bitcoin have no single owner — indeed, they cannot be owned. The purpose of a permissionless ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. This creates censorship resistance, which means that no actor can prevent a transaction from being added to the ledger. Participants maintain the integrity of the ledger by reaching a consensus about its state
Virtualization Layer	The file virtualization layer manages files and file systems across servers. Administrators can then present clients with one logical file mount for all servers.
Wallet	A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.
Wire Transfer	Electronically transferring money from one person to another. Commonly used to send and retrieve fiat currency from bitcoin exchanges.

Annex B

Current State of Blockchain

Distributed ledger technology is any method that shares a system of record across multiple sites and allows participants to enter and/or view data to determine the current state without consulting a central party.

Blockchain is a particular type of distributed ledger technology intended to assure historical integrity and security of transactions by creating a cryptographically secured, tamper-evident record that adds groups of proposed changes to the ledger in successively hash-linked and traceable “blocks” tied into the entire history of ledger entries.

The blockchain innovation has enabled peers to exchange digital representations of value in an immediate and accessible way by building a degree of confidence in the current state of those holdings through a consensus model. This model seeks to eliminate both the reliance on a centralized authority and delays in settlement caused by a third party processor.

The potential to store and exchange real value without an intermediary suggests blockchain use cases extend into many areas traditionally reliant on third-party transaction verifiers. These areas include: payments, audit, brokerage, asset registry, and more. Nonetheless, despite a great deal of work underway, very few projects have progressed beyond proofs of concept in niche use cases. While there is reason to believe that blockchain and distributed ledger technologies as a whole have potential, the current overall state of the technology in 2017 remains uncertain. As innovators explore its potential in diverse use cases and across industries, the technology is still in its nascent stages within financial services, and it faces a number of challenges in order to begin a definitive and orderly path toward widespread adoption.

One important note is that DLTs are associated with a number of technologies including: distributed computing and networking, cryptography and consensus algorithms, notary and time-stamping functions, access control, policy compliance, audit, data confidentiality and participant privacy, etc. All of these components must be functional and effective in order to transform data into useful distributed ledger tools that realistically supports collaboration and exchange of valuable information.

Annex C

Generalized Reference Architecture

The key components of blockchain are a distributed platform for data available for read/write access by a number of peers, and secured through access controls and cryptography in order to ensure a common state of truth. This section provides a generalized description of these blockchain components.

Blockchain System High Level Overview

The below diagram illustrates some basic characteristics of a blockchain system. It is intended to point out the overall participants (system components and people) and principle features.

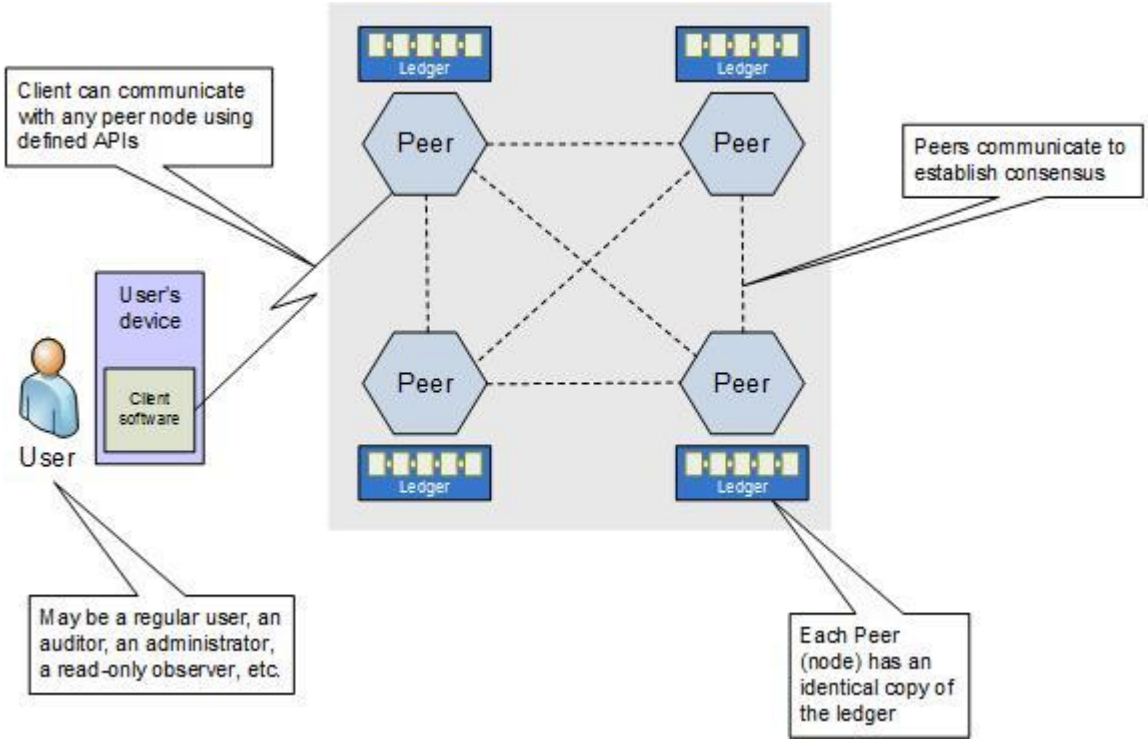

Figure 1 – Blockchain System

Figure 1 illustrates the following elements:

- The blockchain peer nodes, each of which has its own copy of the ledger and related data. In today's blockchains, each node typically has identical capabilities and holds identical data, but other approaches are possible.
- Communication between the peer nodes. Each node communicates with the others in order to verify consensus on any transaction, before writing it to the ledger.

- The end user, who may be a “regular user” who submits requests for blockchain operations, or who may be a special type of user such as an auditor or administrator. All of these users access the blockchain through a set of APIs, using some device running software that interfaces to the blockchain. The device may be a PC, a mobile phone, or anything else capable of executing the necessary software, accessing the network, and interacting with the user.

Blockchain Peer Node in More Detail

The diagram in this section expands on what is happening in a particular peer node.

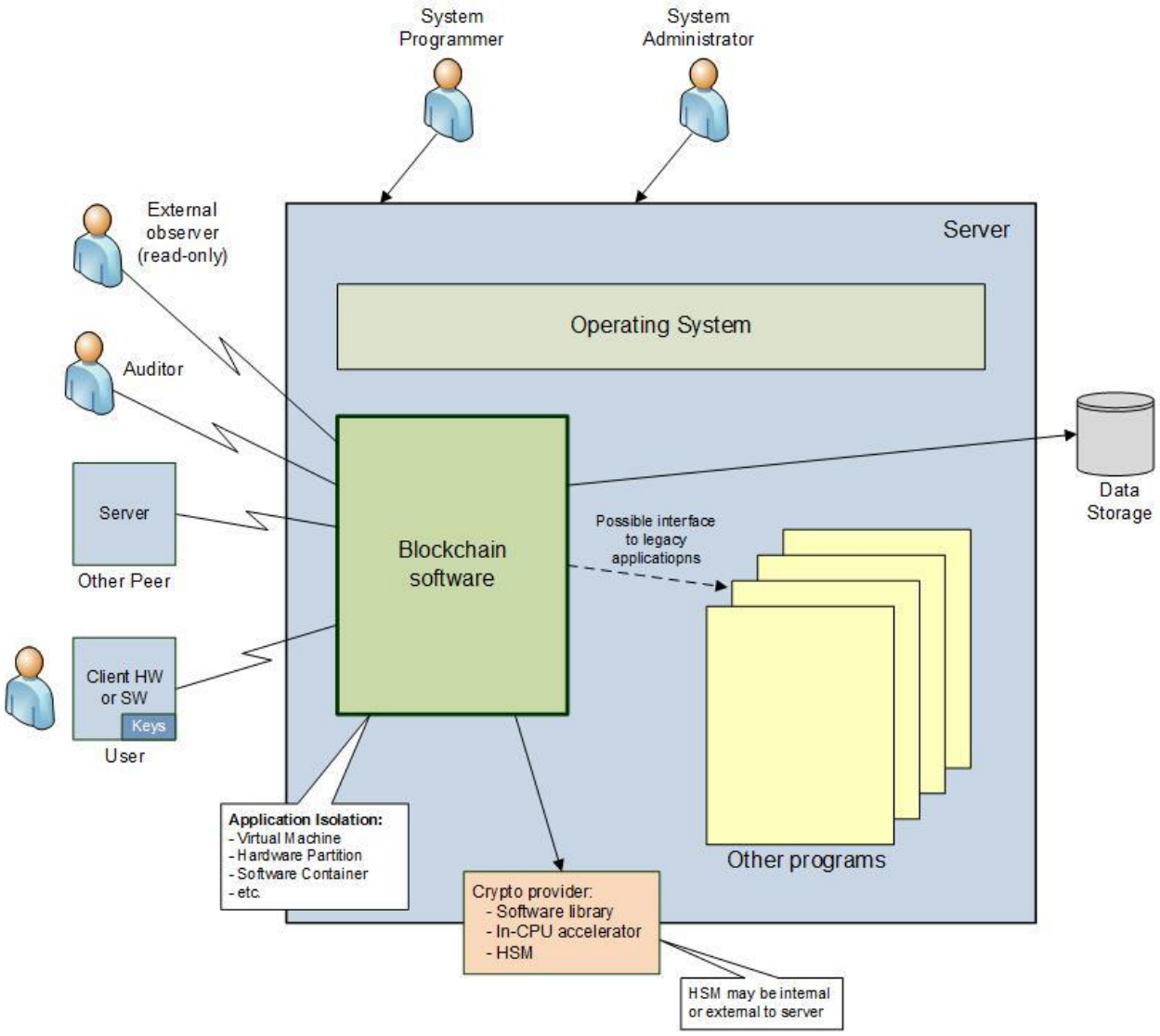

Figure 2 – Blockchain Peer Node

The large blue box represents the server where the peer software is running. It has the O/S, the blockchain software, and some number of other programs. There may also be other components such as virtualization layers. It illustrates that entities of several different types may have access to the system for differing reasons. These entities may include:

- End users who are requesting operations on the blockchain. Their requests are generally authenticated using digital signatures derived from secure private keys.
- Auditors who verify that the system and blockchain meet specified requirements.
- System personnel such as system administrators and system programmers.
- Other blockchain peers, which communicate with this peer for purposes such as consensus on transactions.

Some use cases require interaction between the blockchain and external software such as legacy applications or databases. If this is done, care must be taken to ensure that each peer in the blockchain maintains identical data–this can be difficult, since the blockchain itself is designed to provide that assurance for its own data, but the external applications may not have the necessary characteristics.

Blockchain Software in More Detail

This final diagram shows some of the internal components of the blockchain software. While all blockchain systems share some core characteristics, there are differences in their design and functions.

Note that this diagram introduces *smart contracts*, which was not shown in the previous diagrams. Smart contracts consist of executable code that is contained in the blockchain and can be executed via user or system requests. It can operate on data which is stored separately from the ledger, labelled "smart contract operational data" in the diagram. It is notable that while *smart contract* may imply a particular use for executable code, within the context of blockchains the term is more general and refers to any programming entries supported on the distributed ledger.

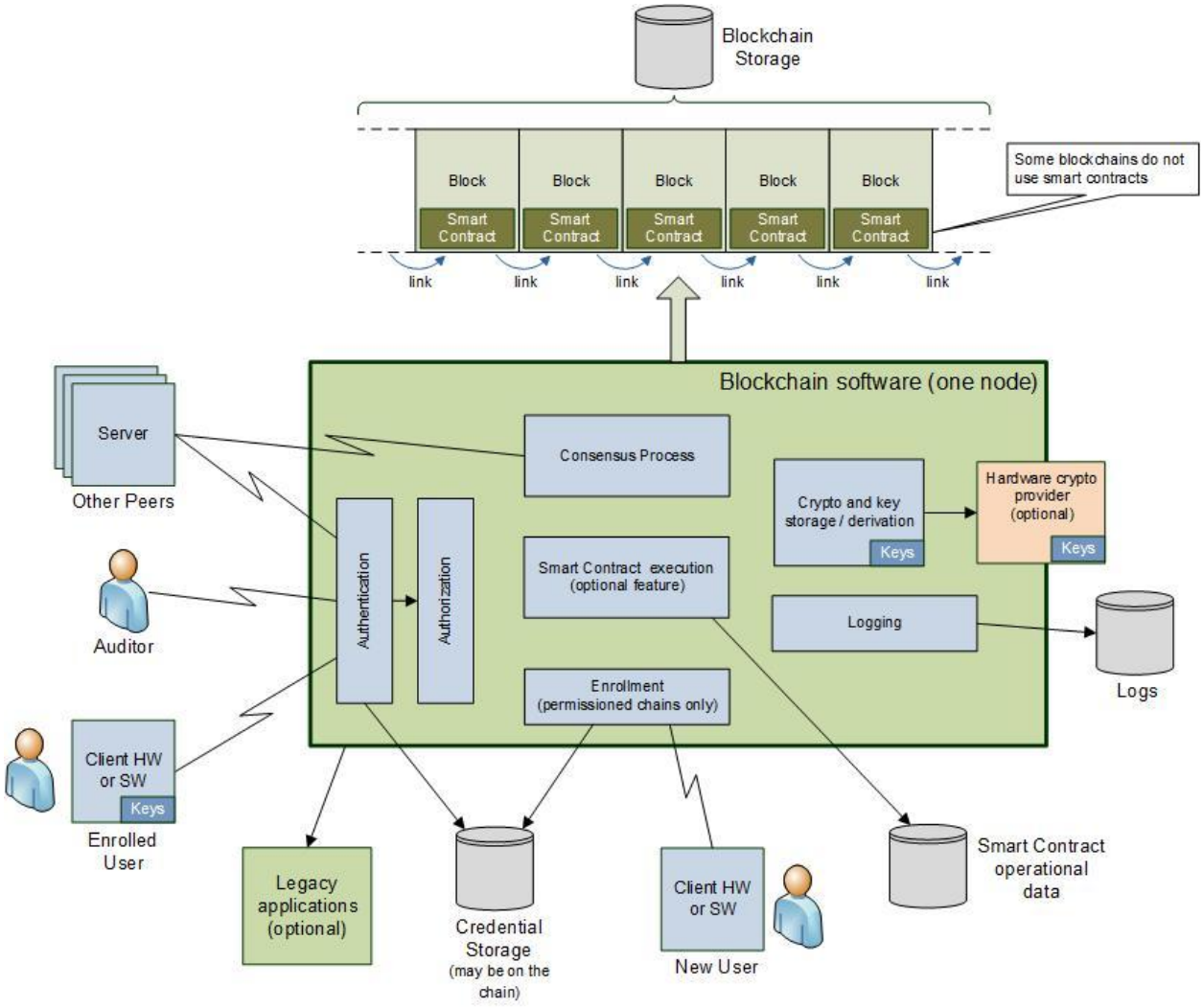

Figure 3 – Blockchain Software

The top of the diagram shows a representation of the blockchain itself, composed of an ordered series of blocks which are linked together in a chain through use of cryptographic hashes. The blockchain is stored on some persistent

storage medium. Optionally, the blocks can contain smart contracts which are installed through user operations. Note that while the smart contracts are logically associated with the blocks, they may be stored separately.

This diagram introduces the access control system. All permissioned blockchains have some form of user authentication and authorization. A traditional access control system is usually provided in which users must be enrolled by an authorized person, and then their credentials are stored so their access rights can be authenticated when they make requests to the blockchain.

Each node in the blockchain system can operate based on a consensus protocol. The consensus process may allow multiple peers to communicate in order to establish confidence that the transaction processing has produced the same results on each peer. The transaction is only committed to the blockchain after successful consensus is reached among peer systems. Some blockchain schemes have pluggable consensus protocols so that the best one can be selected for a particular application, and so that new ones can be used when they are developed.