ASC X9 TR 54–2021

Blockchain Risk Assessment Framework

A Technical Report prepared by:
Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Registered with American National Standards Institute

Date Registered: July 25, 2021

This page intentionally left blank.

Contents

Page

1 Scope, Purpose and Application 1
1.1 Scope and Purpose 1
1.2 Application 3
1.3 Use Cases 3
2 References 3
3 Terms and Definitions 4
3.1 Block 4
3.2 Blockchain 4
3.3 Consensus Protocol 4
3.4 Crypto-asset 4
3.5 Cryptocurrency 4
3.6 Cryptographic Key 5
3.7 Cryptography 5
3.8 Digital Asset 5
3.9 Distributed Ledger Technologies (DLT) 5
3.10 Fork 5
3.11 Immutable 5
3.12 Node 5
3.13 Off-Chain 5
3.14 On-Chain 6
3.15 Oracle 6
3.16 Permissioned 6
3.17 Smart Contract 6
3.18 Stakeholders 6
4 Symbols and Abbreviated Terms 6
5 Risk Assessment Questionnaire 6
5.1 Design and Architecture 7
5.1.1 Data provenance 7
5.1.2 Data integrity 9
5.1.3 Data confidentiality 11
5.1.4 Nodes 11
5.1.5 Modular components 13
5.1.6 Programming languages 13
5.1.7 Code review and maintenance 14
5.1.8 Open source 15
5.1.9 Proprietary systems 16
5.1.10 Smart contract security assessment 16
5.1.11 Inception and execution of smart contracts 17
5.2 Governance and Operations 18
5.2.1 Consensus protocols 19
5.2.2 Governance model 20

5.2.3 Maintenance responsibilities ... 22
5.2.4 Access management ... 23
5.2.5 Jurisdictional laws, regulations, and rules ... 24
5.2.6 Standards ... 24
5.2.7 Change management ... 25
5.2.8 Managed services (hosted) ... 26
5.2.9 Other external blockchain or other distributed networks (multichain) ... 27
5.3 Trust and Resilience ... 28
5.3.1 Cryptographic algorithms ... 28
5.3.2 Public key infrastructures ... 30
5.3.3 Resilience, data persistence, and continuity of operations ... 31
5.3.4 Identity management ... 32
5.4 System Integrations ... 33
5.4.1 APIs ... 34
5.4.2 Interoperability ... 34
5.4.3 External data sources (oracles) ... 35
5.5 Smart Contracts: Legal and Business Processes ... 36

Annex A (Informative) Group Signatures ... 40

Annex B (Informative) Public Key Infrastructures ... 41

Annex C (Informative) Cryptographic Algorithms ... 42

Bibliography ... 43

Foreword

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Committee X9, Incorporated, 275 West Street, Suite 107, Annapolis, MD 21401. This document is registered as a Technical Report according to the “Procedures for the Registration of Technical Reports with ANSI.” 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

This Technical Report is a product of the Accredited Standards Committee X9 Financial Industry Standards and was generated by the X9A3 Subcommittee.

Financial institutions are beginning to build core system architectures using blockchain technology for data storage and processing. The application of this new technology will impact risk assessments and processes for financial accounting, compliance, forensic investigation, and regulatory review.

The introduction of blockchain as part of distributed systems architecture introduces the potential for new end points, vulnerabilities, transaction processing rules, methods for privacy protections, dispute resolution, adherence to governance agreements, and reporting requirements. In addition, the proliferation of different platforms and blockchain designs competing for enterprise-adoption today pose challenges for assessing them. Stakeholders, including design architects, auditors, and other risk assessment professionals will need tools to understand the type of blockchain and its expected capabilities. This work identifies new elements or functions a risk and control assessment may need to address.

Readers may find a baseline understanding of blockchain as a cryptographically secured distributed ledger system important to make best use of this technical report. Throughout this document the terms blockchain and distributed ledger (DLT) are used interchangeably. These considerations may be helpful in supporting both a general understanding of blockchain systems and evaluating the risks:

- **Blockchain is an emerging technology.** The various components may be familiar, but when combined may present unique, unforeseen risks.

- **Many aspects of traditional risk assessments still apply.** Well-known processes like key management, access control, or data integrity evaluations still require attention and assessment, but may also take on additional importance given the new architecture of a blockchain system.

- **Blockchain systems will likely be less flexible than traditional database systems.** In typical traditional databases, risks and controls over the system, and the data it contains, tends to rest with a single authority. However, blockchain systems are distributed by design, which may entail multi-party governance of system updates, emergency changes, and other critical actions. The automation of certain business processes through smart contracts and the expectation of immutability in many blockchain designs may also make it less adaptive. For these reasons, stakeholders may find it more difficult to make necessary technical, compliance, or business rule changes than with a traditional database.

- **Choices in system design should be understood and will result in trade-offs.** Examples include:
    - performance may be lower if security is higher;
    - recording data meant to be immutable has both risks and benefits;
    - using open-source code has advantages, but can be more difficult to manage where bug fixes or updates are needed; and
    - using a software provider or consultant services may be more cost-effective up front but could result in challenges when updates are needed to the system.

- **New technologies relevant to blockchain are being introduced all the time.** New consensus mechanisms, programming languages, system designs, encryption options, privacy protection mechanisms, etc. are all in a rapidly evolving state with no clear winner in sight.

- **Consensus standards to support audit, risk assessment, and interoperability considerations are under development, but are not yet widely available.** In parallel with this work**,** the International Organization for Standardization (ISO) continues to work on auditing considerations, security, and interoperability questions, though not necessarily specific to financial services or payments.

This document leverages traditional risk assessment practices currently in use and extends them to incorporate blockchain and distributed ledger technologies.

Suggestions for the improvement or revision of this Technical Report are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 275 West Street, Suite 107, Annapolis, MD 21401 USA.

This Technical Report was processed and registered for submittal to ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Technical Report does not necessarily imply that all the committee members voted for its approval.

At the time this Technical Report was published, the X9 committee had the following members:

Roy C. DeCicco, X9 Chairman
Corby Dear, X9 Vice Chairman
Steve Stevens, Executive Director
Janet Busch, Program Manager
Ambria Frazier, Program Manager

Organization Represented	***Representative***
ACI Worldwide	Doug Grote
Amazon	Igor Kleyman
American Bankers Association	Diane Poole
Bank of America	Daniel Welch
BankVOD	Sean Dunlea
BDO	Tim Crawford
Bloomberg LP	Corby Dear
Communications Security Establishment	David Smith
Conexxus, Inc.	Gray Taylor
CUSIP Global Services	Gerard Faulkner
Delap LLP	Andrea Beatty
Deluxe Corporation	Andy Vo
Diebold Nixdorf	Bruce Chapa
Digicert	Dean Coclin
Discover Financial Services	Diana Pauliks
Dover Fueling Solutions	Henry Fieglein
Federal Reserve Bank	Ainsley Hargest
FirstBank	Ryan Buerger
FIS	Stephen Gibson-Saxty
Fiserv	Lisa Curry
Fiserv	Dan Otten
FIX Protocol Ltd - FPL	James Northey
Futurex	Ryan Smith
Gilbarco	Bruce Welch
Harland Clarke	Jonathan Lee
Hyosung TNS Inc.	Joe Militello
IBM Corporation	Richard Kisley
Ingenico	Steven Bowles
ISITC	Lisa Iagatta
ITS, Inc. (SHAZAM Networks)	Manish Nathwani

J.P. Morgan Chase	Roy DeCicco
MagTek, Inc.	Mimi Hart
MasterCard Europe Sprl	Mark Kamers
NACHA The Electronic Payments Association	George Throckmorton
National Security Agency	Mike Boyle
NCR Corporation	Kevin Spengler
Office of Financial Research, U.S. Treasury Department	Thomas Brown Jr.
PCI Security Standards Council	Troy Leach
PricewaterhouseCoopers LLP	Michael Versace
SWIFT/Pan Americas	Karin DeRidder
Symcor Inc.	Debbi Fitzpatrick
TECSEC Incorporated	Ed Scheidt
The Clearing House	Sharon Jablon
U.S. Bank	Michelle Wright
U.S. Commodity Futures Trading Commission (CFTC)	Robert Stowsky
University Bank	Stephen Ranzini
USDA Food and Nutrition Service	Lisa Gifaldi
VeriFone, Inc.	Joachim Vance
Viewpointe	Richard Luchak
VISA	Kristina Breen
Wells Fargo Bank	Sotos Barkas
Zions Bank	Kay Hall

At the time this Technical Report was published, the **X9A Electronic and Emerging Payments subcommittee** had the following members:

Guy Berg, Chairman

Organization Represented	***Representative***
American Bankers Association	Steven Kenneally
American Bankers Association	Tab Stewart
American Express Company	Gail Chapman
Bank of America	Andi Coleman
Bank of America	Sean Fitzpatrick
Bank of America	Michael Shanzer
Bank of America	Matt Sharp
Bank of America	Daniel Welch
Bank of America	Terri Willis
CDP, Inc.	Johnny Sena
Conexxus, Inc.	Alan Thiemann
Conexxus, Inc.	Linda Toth
Delap LLP	Andrea Beatty
Diebold Nixdorf	Bruce Chapa
Discover Financial Services	Diana Pauliks
Dover Fueling Solutions	Henry Fieglein
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Patti Ritter
Federal Reserve Bank	Scott Brubaker
Federal Reserve Bank	Marianne Crowe
Federal Reserve Bank	Ainsley Hargest
Federal Reserve Bank	Brooke Imhoff
Federal Reserve Bank	Raphael Johnson
Federal Reserve Bank	Angela Lawson

Federal Reserve Bank	David Lott
Federal Reserve Bank	Susan Pandy
Federal Reserve Bank	Raven Dampier
FIS	Prashant Gupta
FIS	Cary Jeffers
FIS	Gail Lumsden
FIS	Prajoy Prabhakaran
FIS	Joe Stein
Fiserv	Lisa Curry
Fiserv	Kelly Hynek
Fiserv	Dan Otten
Gilbarco	Bruce Welch
Health and Human Services Commission	Duane Grabarschick
Health and Human Services Commission	John Hannemann
Inmar	Joyce Ballack
Inmar	Cameron Clark
Inmar	Taquanica Floyd
Inmar	Poovannan Rathinam
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Clinton Jones
MasterCard Europe Sprl	Carl Jansson
MasterCard Europe Sprl	Vince Morelli
NCR Corporation	Jackie Farone
NCR Corporation	Rick Fender
NCR Corporation	Stephen Gawne
NCR Corporation	Bradford Loewy
NCR Corporation	Scott Meier
Office of Financial Research, U.S. Treasury Department	Jennifer Bond-Caswell
P97 Networks, Inc.	Donald Frieden
P97 Networks, Inc.	David Nichamoff
PricewaterhouseCoopers LLP	Michael Versace
SWIFT/Pan Americas	Karin DeRidder
Symcor Inc.	Debbi Fitzpatrick
TECSEC Incorporated	Jay Wack
Thales UK Limited	Amit Sinha
The Clearing House	Sharon Jablon
The Clearing House	Jackie Pagán
University Bank	Stephen Ranzini
University Bank	Michael Talley
USDA Food and Nutrition Service	Lisa Gifaldi
USDA Food and Nutrition Service	Erin McBride
Viewpointe	Richard Luchak
VISA	Glenn Powell
Wells Fargo Bank	Gagandeep Bakshi
Wells Fargo Bank	Sotos Barkas
Wells Fargo Bank	Debbie Chacon
Wells Fargo Bank	Paul Crofts
Wells Fargo Bank	Jeff Fromm
Wells Fargo Bank	Joe Janas
Wells Fargo Bank	Rameshchandra Ketharaju
Wells Fargo Bank	Alan Nguyen
Wells Fargo Bank	Mark Schaffer

Wells Fargo Bank	Jeff Stapleton
Wells Fargo Bank	Anita Sukur
Wyoming Department of Health WIC Program	Wes Cure
Wyoming Department of Health WIC Program	Tina Fearneyhough
Wyoming Department of Health WIC Program	Melissa Sosa

Under ASC X9, Inc. procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or guideline(s) in a specific area and is then disbanded. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or guideline. (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 Technical Report was published, the **X9A3 Blockchain Auditing Working Group**, which developed this technical report had the following active members:

Michael Versace, Chairman
Angela Lawson, Vice Chairman

Special Acknowledgement *– this technical report and the ongoing efforts of X9A3 are dedicated to the lifelong contributions of our colleague Philip Griffin.*

Organization Represented	***Representative***
American Bankers Association	Steven Kenneally
American Bankers Association	Samantha Pelosi
Bank of America	Andi Coleman
Bank of America	Michael Shanzer
Bank of America	Daniel Welch
BDO	Maurice Liddell
BDO	Greg Schu
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Angela Lawson
Federal Reserve Bank	Skyler Pinna
FIX Protocol Ltd - FPL	James Northey
Gilbarco	Bruce Welch
ITS, Inc. (SHAZAM Networks)	Misty Trimble
National Security Agency	Jerome Vacek
PricewaterhouseCoopers LLP	Michael Versace
Wells Fargo Bank	Andrew Garner
Wells Fargo Bank	Jeff Stapleton
Wells Fargo Bank	Tony Stieber
Wells Fargo Bank	Anita Sukur
Wells Fargo Bank	Sean Zhang

Blockchain Risk Assessment Framework for Permissioned Systems

1 Scope, Purpose and Application

1.1 Scope and Purpose

This technical report (TR) provides a framework for the performance of operational risk assessments on blockchain systems and applications within a distributed network. Operational risks include information technology (IT) and information security (IS) areas. IT includes interoperability, resiliency, accessibility, and software maintenance. IS includes data integrity, confidentiality, authentication, authorization, and accountability (logging capability). This report features some aspects of application risks including data accuracy, version control, backwards compatibility, and other usability functions.

This technical report can be used for multiple purposes, including system design reviews, internal control planning, or internal and external audits. Risk assessments are a basic and necessary function for providing blockchain assurance to stakeholders.

The content of this document is intended to provide the reader with background terminology and concepts of a blockchain system. This document's main contribution is the Risk Assessment Questionnaire (Section 5.). Here, we offer a series of questions for identifying the blockchain environment and potential risks, and a set of high-level IT control objective statements. The framework, questionnaire, and IT controls are use case-agnostic and oriented to permissioned blockchain systems.[1] The Risk Assessment Questionnaire is divided into five main categories. Each main category (see below) contains several subsections, as described in Table 1.

Design and Architecture: *Discovers the risks of the system's design and architectural arrangement.*

Governance and Operations: *Discovers the risk of how the system technically operates and how technical functions are governed.*

Trust and Resilience: *Discovers the risks of inadequate technical security processes*

System Integration: *Discovers the risks of integration points outside the blockchain system itself.*

Smart Contracts: Legal and Business processes: *Discovers the risks of autonomous/technical execution of activities based on the fulfilment of pre-agreed conditions described in written/traditional contracts.*

[1] Note that a 'permissioned' system is one in which some control and governance, established by agreement of the parties participating in the system, exists to determine who or what is allowed to read, write, or in other ways manage, operate, or govern the system. Some blockchain systems are public and considered 'permissionless' such that anyone with the requisite hardware, software, and skill can participate in all or most activities of the network. These types of systems may introduce additional risks beyond the scope of this report.

Table 1: Main sections and corresponding subsections within the Risk Assessment Questionnaire

Main Sections	**Design and Architecture**	**Governance and Operations**	**Trust and Resilience**	**System Integrations**	**Smart Contracts: Legal and Business Processes**
Subsections	Data provenance	Consensus protocols	Cryptographic algorithms	APIs	
	Data integrity	Governance	Public key infrastructures	Interoperability	
	Data confidentiality	Maintenance responsibilities	Resilience, data persistence and continuity of operations	External data sources	
	Nodes	Access management	Identity management		
	Modular components	Jurisdictional laws, regulations, and rules			
	Programming languages	Standards			
	Code review and maintenance	Change management			
	Open source	Managed services (hosted)			
	Proprietary systems	Other external blockchain or other distributed networks (multi-chain)			
	Smart contract security assessment				
	Inception and execution of smart contracts				

The content of this document does not include detailed audit plans or the detailed controls and test of controls that are required when designing an audit plan. The content from this document can be leveraged by the reader when assessing risks and determining what components may be needed within the audit plan. It is recommended that the reader review blockchain-oriented audit plans, audit guidance or relevant information that may be available from the following organizations:

- American Institute of Certified Public Accountants (AICPA) - https://www.aicpa.org/

- Canadian Institute of Chartered Accountants (CICA) – https://www.cpacanada.ca/
- Information Systems Audit and Control Association (ISACA) - https://www.isaca.org/
- The Institute of Internal Auditors (IIA) - https://na.theiia.org/Pages/IIAHome.aspx

In addition, several other topics are considered out of scope for this technical report but are highly recommended for future study. These include.

- Data and process operations performed off the blockchain. This would include off-chain data provenance, integrity, and confidentiality business process and operations.
- Specific capabilities necessary to judge the authenticity of an input document to the blockchain. For example, this technical report does not address the usefulness, completeness, truthfulness, or accuracy of data or documents input to the blockchain system.
- Specific technical considerations for providing assurance over data or processes supporting blockchain operations but performed off-chain.
- Credit and/or market risks associated with the application of blockchain technologies or consensus mechanisms may apply, depending on the scope of the specific blockchain application under consideration.

1.2 Application

Financial institutions are beginning to use blockchain for various applications, such as issuing letters of credit, reducing manual documentation processes in trading activity, crypto (or digital) -asset custody, stablecoin or other cryptocurrency payment activity, and managing data shared with multiple parties. Major financial institutions are partnering together with consortium groups to investigate the potential for blockchain in their operations and business practices. A blockchain alone is not a platform, rather it is often used as a component within a larger system. For this reason, many standard security and risk assessment practices may still apply. However, where a blockchain interacts within legacy systems, or where it introduces a new method for achieving a certain result, auditors need a practical guide to understand what to look for to perform an accurate assessment and request the right data.

1.3 Use Cases

This report notes two main categories of use cases for the application of blockchain systems within financial services.

- Tracking changes, sometimes known as “state changes,” to information needed by multiple parties such that each party has access to the most up-to-date data and can trace the origin of the input without a centralized processing hub
- Facilitating value exchanges, including payment activities, among a community of participants without a centralized processing hub

Defining the risk of a permissioned blockchain starts with understanding the specific use case. For example, a blockchain implementation that records only a hash reference to documents maintained in a separate database will have a significantly different risk profile than a blockchain implementation intended to transfer and record value exchanges. The risk assessment provided in this report applies to both use cases unless otherwise noted.

2 References

The following referenced documents are helpful for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2.1 ISO 21188:2018 Public key infrastructure for financial services – Practices and policy framework

2.2 X9.138:2020 Distributed Ledger Technologies (DLT) Terminology

2.3 X9.95-2016 Trusted Time Stamp Management and Security

2.4 Committee on National Security Systems Instruction (CNSSI) No. 4009 (April, 2010)

2.5 NIST Special Publication (SP) 800-63 Digital Identity Guidelines (June, 2017)

2.6 X9.73:2017 Cryptographic Message Syntax (CMS) – ASN.1 and XML

2.7 ISO 23576:2021 Blockchain and distributed ledger technologies — Security management of digital asset custodian

3 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

3.1 Block

a set of data representing a confirmed batch of transactions with an associated header containing a timestamp hash-linked to the previously confirmed set of data which ensures the continuity of a ledger

[SOURCE: X9.138:2020, 3.1]

3.2 Blockchain

a type of distributed ledger technology that groups data into blocks that are (i) hash-linked chronologically and are confirmed by a consensus mechanism over a shared distributed network of participants to validate the creation of transactions or events being posted to the ledger and (ii) is tamper-resistant and intended to serve as an immutable record of all such transactions and events

[SOURCE: X9.138:2020, 3.2]

3.3 Consensus Protocol

a system of agreement that allows a collection of distributed participants to affirm transactions that can be recorded to the shared ledger

[SOURCE: X9.138:2020, 3.7]

3.4 Crypto-asset

any digital asset that relies on aspects of cryptography and distributed ledger technology for its issuance, storage, exchange, or transaction validation, including, but not limited to, cryptocurrencies, crypto-securities, and utility tokens

[SOURCE: X9.138:2020, 3.8]

3.5 Cryptocurrency

a digital currency that (i) does not have legal tender status, (ii) is or is not intended to be used as a medium of exchange, (iii) is not a security under the appropriate government authority, and (iv) relies on aspects of cryptography and distributed ledger technology to be issued, transferred, stored or traded electronically

[SOURCE: X9.138:2020, 3.8]

3.6 Cryptographic Key

value used in *cryptographic* operations, such as decryption, encryption, signature generation, or signature verification

[SOURCE: SP 800-63]

3.7 Cryptography

discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof

[SOURCE: ANSI X9.95:2016, 3.16]

3.8 Digital Asset

an electronic representation of value

Note: for the purposes of this document, the terms digital asset and crypto-asset are used interchangeably

[SOURCE: X9.138:2020, 3.15]

3.9 Distributed Ledger Technologies (DLT)

a digital recordkeeping system, governed by rules and/or a consensus mechanism, where information is replicated across multiple sites or entities

[SOURCE: X9.138:2020, 3.18]

3.10 Fork

two or more *blocks hash-linked* to the same preceding *block*

[SOURCE: X9.138:2020, 3.19]

3.11 Immutable

design feature such that the potential for alteration of finalized data without detection is negligible

3.12 Node

an entity with established authorities in a blockchain through the execution of roles and hierarchical relationships. There are multiple types of nodes, including supervisory nodes, which give the ability to monitor, audit, and keep account of all activity on a blockchain.

Note: typically, a computational node, i.e. some combination of hardware/software that “participates” in the blockchain system

3.13 Off-Chain

data and data processing activity that occurs outside of a blockchain’s protocols and ledger

3.14 On-Chain

data and data processing activity that occurs on the blockchain and is governed by the blockchain's technical capabilities, protocols and consensus processes

3.15 Oracle

the source of external data written to a ledger used to inform a decision or an action on that ledger

[SOURCE: X9.138:2020, 3.25]

3.16 Permissioned

restrictions on a participant's ability to read or write data

Note: restrictions may include the use of authentication, authorization, or cryptography

[SOURCE: X9. 138:2020]

3.17 Smart Contract

computer code and supporting processes on a blockchain that automatically executes, based on some event or condition, according to predetermined agreement

3.18 Stakeholders

those who design blockchain systems, provide business requirements, quality control or assurance responsibilities, or any other interested party

4 Symbols and Abbreviated Terms

For the purposes of this document, the following symbols and abbreviations apply.

AML	Anti-Money Laundering
API	Application Programming Interface
CFT	Combating the Financing of Terrorism
DLT	Distributed Ledger Technologies
NIST	National Institute for Science and Technology

5 Risk Assessment Questionnaire

Each section below includes a short introduction to illustrate what may be new or different in a blockchain system versus a traditional ledger or database structure. These introductions also provide context which may help reduce ambiguity for readers and spur additional questions for future discussions. The main sections are as follows: Design and Architecture, Operations and Governance, Trust and Resilience, System Integration, Third Party, and Smart Contracts: Legal and Business Processes. Each main section contains an overall control objective statement. Sub-sections describe various aspects of the main section and include both a control objective specific to the sub section and a list of questions. Each set of questions is intended to support stakeholders towards the discovery of the specific risks of the blockchain or surrounding system they may be considering.

5.1 Design and Architecture

The design and choice of architecture varies by blockchain implementation and use case. Considerations described below are generally applicable to most, though not all, blockchain implementations. One key aspect to understanding the risk profile of any technical assessment includes diagramming and understanding the system and explaining each physical or virtual aspect of the system, including external dependencies.

When planning or assessing the architecture and design of a system, stakeholders should also understand the data flow, storage, infrastructure, network controls, routing capabilities, and inventory of hardware and software. An end-to-end system review and understanding at the appropriate authority level prior to implementation is a best practice in assessing the risks in any information system. This section highlights architecture and design questions related to core components common to most permissioned blockchain systems.

To assess the integrity of a blockchain system, stakeholders may need to understand if any elements of the system are designed to be changed without disruption to the core system. Highly modular architectures can separate the application layer from the core system such that components such as consensus algorithms or business rules can be customized specific to a particular business need. A developer could use a different programming language from the underlying core system, for example, without affecting the overall functioning of the system.

Design and Architecture includes the following subsections:

- Data provenance
- Data integrity
- Data confidentiality
- Nodes
- Modular components
- Programming languages
- Code review and maintenance
- Open source
- Proprietary systems
- Smart contract security assessment
- Inception and execution of smart contracts

> **Design and Architecture overall control objective** – The design and architecture of the blockchain solution is understood and documented sufficiently to support business process, data, and IT control requirements. This control objective should be considered in addition to control objectives in each Subsection below.

5.1.1 Data provenance

A defining feature of blockchain includes the immutable recording of transactions and events once the information is either generated by the system itself or added and confirmed through the consensus process. Where the data originates will affect the verifiability of its provenance. Because trust considerations, consensus mechanisms, and verifiability of data may differ if the data originated on-chain or was delivered to the blockchain system by an external system, stakeholders should understand the provenance of data recorded on a blockchain. This section focuses on the origin of data and how it is moved into transactions recorded on the ledger.

> **Data provenance control objective:** The enterprise has adequate controls to ensure that the ownership, origin, and lineage of on-chain and off-chain data is known and maintained throughout the data lifecycle.

The following risk assessment questions should be considered:

Data provenance questions:	
1	What is the original source(s) of the transaction data recorded on the blockchain? ● What is the data flow and is it documented? ● Does the data flow documentation include any third-party vendors?
2	If the blockchain is storing the location of off-chain data, such as the location of documents, but not the documents themselves then: ● What are the off-chain sources of data and how does the data flow? o Is this included in documentation of the data flow? ● How is the off-chain data controlled, and any changes subsequently synchronized for all affected nodes? (e.g. the use of hashing to control versioning or state)
3	Is it possible to generate and record on-chain data without going through a transaction? (For example, some systems may allow smart contract code to assemble and validate data from an off-chain system prior to the updated state of the contract being recorded) ● If yes, what is the process? ● Is this included in the documented data flow?
4	Is provenance verification performed on every piece of data coming into every transaction recorded on the blockchain? ● If no, what are the exceptions? ● If yes, how is the provenance verification performed?
5	Can an audit trail trace end-to-end ownership control of an asset?
6	Does the process involve methodologies such as zero-knowledge proofs or other mechanisms that may affect the ability to determine the origin authenticity of data on the chain?
7	If external data is used in a transaction, how trustworthy is the source? How is its trustworthiness continuously monitored and justified?
8	If external data is used in a transaction, what verification process is implemented to ensure consensus.
9	During provenance verification, is there any potential of third-party data leak[2]?

[2] Third-party data leak occurs when the transaction history of the primary parties is exposed to another party who was not a participant of the past transactions.

5.1.2 Data integrity

Many consider the ‘immutability’ of a blockchain’s transaction history an important feature of a blockchain system. When stakeholders intend the data to be immutable, the accuracy of data recorded on-chain and the ability to verify it gain importance. Stakeholders may wish to consider any pre-specified exceptional circumstances before implementation of the system (such as the scenarios identified in the Data provenance section). Likewise, stakeholders should take note of where or how corrupt and/or malicious data could enter the chain. This section focuses on the maintenance and assurance of accuracy and consistency of data recorded on the blockchain. This includes validation processes to ensure the quality of the data and that it is correct and useful.

> **Data integrity control objective:** The blockchain has adequate controls that provide reasonable assurance over the integrity of on-chain data and the transactions are maintained and known throughout the data lifecycle.

The following risk assessment questions should be considered:

Data integrity questions:	
1	How is data formatted and what encoding rules are used? Is it consistent among all participating parties that interact with the blockchain or will a transformation/translation process need to occur? • If a transformation occurs, what are the mechanisms and controls?
2	What is the interaction between off-chain, on-chain, and physical or virtual goods? If the blockchain contains references to off-chain data or refers to physical or virtual goods, such as a plot of land or the right to access certain media, rather than the data itself, what protocols are in place to assure that these references are valid? ● If an asset is represented by a digital token, how does the tokenization process ensure the physical asset is tokenized no more than once (double-spend problem)? ● What is the settlement risk of digital assets against real? ● Can an assessment or audit trail trace end-to-end ownership control of an asset? ● When is ‘ownership’ determined**?** ● How is timing of ownership transfer managed?
3	What prevents corrupted, fraudulent, or otherwise inaccurate data from entering the chain?
4	How is data, once added to the chain, protected from deletion or corruption?
5	If a cryptographic or digital signature attests to transaction data, what specific data is the signature committing to? ● Is unsigned data mutable? Could a change to this data materially affect the transaction record stored on-chain?

Data integrity questions:	
	● Is unsigned or partially signed transaction data populated to the chain? ● Whose signature(s) are required on the transaction? ○ How is that requirement enforced? Is there a mechanism for monitoring and/or alerting relevant parties to changes to recorded data via new entries recorded to the blockchain?
6	Under what conditions, if any, is data allowed to be changed or deleted? (E.g. spam, inappropriate information, mistaken recipient, legal requirement, etc.) ● What alterations can be made by what entity with what access level? ● How are those rules enforced? ● What is the process for alteration/deletion?
7	If a private or symmetric key assigned to a particular user was lost or stolen, what prevents adding its signed transactions to the chain? • If such a prevention mechanism is in place, how does it operate?
8	What controls exist to detect man-in-the-middle attacks between blockchain and off-chain data transfers?
9	When is a transaction considered final? ● How will disputes be handled where the validity of transactions considered final by the system are questioned?
10	Do transaction ordering or other processes within the system require a timing server or timestamp mechanism? • Do all nodes in the network draw from an authoritative time source? Do adjacent external systems draw from this same time source?
11	Does the system involve methodologies such as zero-knowledge proofs or other mechanisms that may affect the ability to determine the origin authenticity of data on the chain?
12	How does a party recover partially or completely lost data to maintain data integrity? (e.g. Has this been addressed in a business continuity plan?)
13	How does the company’s data retention policy impact data integrity?

5.1.3 Data confidentiality

Because data stored on a blockchain is often difficult to modify or remove, stakeholders should thoroughly understand the type of data recorded. Similar to traditional databases, stakeholders should also be aware of any sensitive or regulated data which might be stored, as this may affect design considerations and access restrictions. This section focuses on the processes and rules that limit access or places restrictions on use.

> **Data confidentiality control objective**: The blockchain has adequate controls that provide reasonable assurance over the confidentiality of on-chain data. Though individual contributors may not be known, there is governance over authorized roles. Additionally, there is awareness of the sensitivity of the data that can be stored on the blockchain and how it should be handled.

The following risk assessment questions should be considered:

Data confidentiality questions:	
1	What types of data will the blockchain system hold?
2	What is the security classification of the data?
3	Is personally identifiable information (PII) or other sensitive data included?
4	Is the blockchain data covered by any rules based on legal or regulatory considerations?
5	What mechanisms are responsible for adherence to or enforcement of these rules?
6	How are access and authority rules defined and enforced?
7	How is transaction privacy enforced?
8	Who can encrypt and decrypt data?

5.1.4 Nodes

A blockchain is a network of nodes which participate in consensus protocols and collectively maintain a decentralized database.[3] In a permissioned blockchain, nodes represent known entities with established identities. Nodes are instances of software that perform activities necessary for the operation of the blockchain. In a blockchain system, nodes may perform the same functions, which would typically include reading and writing data to the blockchain as well as some form of verification that other participants have followed the protocols established by the system. However, different blockchain systems may have special nodes that perform specific types of functions. Understanding what each node or type of node in the system is designed to do, what functions it supports and the

[3] In systems like Bitcoin, Ethereum, etc., nodes do not have to participate in consensus to be a node in the network –a "light" node can run that only looks for and validates transactions related to particular wallet addresses or even run a full node but not participate in mining / staking (consensus). However, in most permissioned networks all nodes participate in consensus processes.

rules that govern its behaviour is important to assessing the risk each node presents to the system as a whole (See Governance and Operations and Consensus).

> **Nodes control objective:** The blockchain has adequate controls that provide reasonable assurance that node ownership roles and node functions, particularly as these functions relate to risk management and control, are understood and documented.

The following risk assessment questions should be considered:

Nodes Questions:	
1	Does any single node have greater control or have different functions than others? These functions may include: • Routing and access controls • Managing business rules • Monitoring system activity, health or performance • Monitor linkages between on and off-chain data • Perform reporting tasks • Generate alerts • Ordering and submitting blocks • Validate or confirm blocks and transactions • If so, what are the various functions and how are they implemented and controlled? Are they documented? Based on the function, how will performance of this function be monitored and assessed?
2	What procedures are in place to address the failure or breach of a node on network? What are the response and remediation procedures?
3	What mechanisms are used to assure the authenticity of the node?
4	Who owns the nodes? • What are the responsibilities of ownership? • Where are they located? • Who has responsibility for node management? • What are the management responsibilities?
5	How are new nodes in the network: • Authorized? • Added to (or deleted from) the network?
6	What are the update procedures for maintenance of authorized nodes? • What control procedures are in place to ensure node maintenance is authorized?

5.1.5 Modular components

To assess the integrity of a blockchain system, stakeholders may need to understand if any elements of the system are designed to be changed without disruption to the core system. Highly modular architectures separate the application layer from the core system such that components such as consensus algorithms or business rules can be customized specific to a particular business need. Software design best practices favor a “high cohesion, loose coupling” design in which single-function modules (e.g. encryption algorithms) are tightly encapsulated and referenced by other modules, which allows for easier maintenance as components are upgraded/deprecated. Additionally, a developer could use a different programming language from the underlying core system.

> **Modular components control objective:** The blockchain has sufficient controls to maintain the continuity and integrity of approved operations as changes are planned, tested, and introduced.

The following risk assessment questions should be considered:

Modular components questions:	
1	Are there modular components? ● If so, what can be swapped in or out? ● How does the swap occur? ● What is performed prior to and after a component is added, removed or updated?
2	Is there sufficient separation among design components such that modules can be changed with relative ease and minimal impact to unrelated code?

5.1.6 Programming languages

While there are differences in query languages used for traditional databases, generally these differences are small, and the languages are both established and understood. This may not be the case in blockchain systems, where programming languages are rapidly evolving, and subsequently may pose development risks.

> **Programming languages control objective:** Programming languages used to construct blockchain functions and operations are appropriate for use, under change control, and supported by reference architecture or technical design standards.

The following risk assessment questions should be considered:

Programming language questions:	
1	What programming languages are used within the blockchain system? ● How well-understood is the programming language? Could a developer with knowledge of this language be readily accessed for updates or needed changes?

Programming language questions:	
	● Are there technical design standards, that indicate appropriate programming languages, versions, and other design elements suitable for use?
2	What kinds of on-chain operations does the programming language allow for?
3	Has the programming language used for the blockchain solution been reviewed for suitability for the intended applications? • Have any limitations been identified and documented? • If limitations exist, has suitability of the programming language been reviewed and limitations addressed in light of these limitations?

5.1.7 Code review and maintenance

The best practice for code development in general includes a security assessment of the code prior to publishing or deployment; stakeholders may want to employ the same practice for code used to develop the blockchain, including smart contracts. Firms employing smart contracts to handle high-value transactions may seek to be especially vigilant.

Software runs the blockchain as almost everything else in the modern world. The blockchain, due to its decentralized nature and diminished/relaxed constraint on trust, has an added need for transparency of the development and maintenance of the underlying source code. That is one of the major reasons why most of the prevailing blockchain projects are or will be open sourced. At the same time, blockchains with proprietary source code exist to serve niche/specialized markets. Whether the source code is open source or proprietary will have different considerations for maintenance. The following sections highlight those considerations stakeholders may want to review to understand risk and to assess the need for any additional control or caution.

> **Code review and maintenance control objective**: Code security assessments and penetration tests are performed on all blockchain code prior to implementation and on a routine basis. Internal controls exist to ensure the maintenance of the blockchain's underlying code is well-understood and suitable for the given business need.

The following risk assessment questions should be considered:

Code review questions:	
1	Who performed the code security assessment? • Is there adequate separation of functions between code reviewers, quality assurance, and operations?
2	What is the origin of the code? (see Open Source section 5.1.8 and Proprietary Systems 5.1.9)
3	Have any known backdoors been addressed?
4	How is the system codebase managed?

Code review questions:	
5	What code reviews have been done? ● Were the reviews documented? ● Who has reviewed the risks and accepted them?
6	Has application penetration testing been performed?
7	Does the expertise on the code reside in-house or depend on consultants or others for the management of the code? ● If using outside developers or consultants, how will new code development be handled? ● If in-house, have intellectual property agreements been signed by in-house developers?

5.1.8 Open source

An open source blockchain provides total visibility of its underlying protocols and promises high quality codebase and clear documentation. The open source community has a transparent governance structure, code quality standard, code maintenance policy, and revenue and license model. Stakeholders should seek to fully understand their implications on feature availability, service and support, and compatibility and forking potentials.

> **Open source control objective**: The benefit and risk of using open sourced software within a blockchain system is explicitly evaluated.

The following risk assessment questions should be considered:

Open source questions:	
1	Has legal review of open source implications occurred and does the use of open source comply with organizational standards and policies? ● Do contributors have any liability? ● Are the licensing terms appropriate for use in the blockchain solution?
2	How are modifications to the underlying code managed? ● Will modifications to the source code cause incompatibility issues for incorporating bug fixes? ● What is the merge process for code changes, and how are any changes tracked?
3	What are the rationales for choosing to rely on an open source blockchain? ● Are the reasons well suited and appropriate for the given business need?
4	Has the open source code been audited to ensure it executes as laid out in written specifications?

Open source questions:	
	● To what extent was the audit conducted and how recently? ● What is the reputation and experience of the auditor?

5.1.9 Proprietary systems

Proprietary systems, also referred to as closed source, refers to blockchains in which the source code is not shared with the public. Instead, in a proprietary blockchain, a centralized third party is responsible for maintaining, accessing, and upgrading the underlying code that governs the blockchain.

> **Proprietary systems control objective:** Proprietary components used within a blockchain system are appropriate based on the defined use of the system and include applicable governance and management oversight.

The following risk assessment questions should be considered:

Proprietary systems questions:	
1	Who is the third party responsible for maintaining the blockchain?
2	Are there any contingencies in place in the event of the propriety blockchain no longer being supported by the controlling third party?
3	Is the proprietary blockchain a fork of an existing public blockchain?
4	Does the proprietary blockchain provide the ability to interoperate with any public blockchains?
5	Does the third party in control of the proprietary blockchain have any ability to access data shared across the network?
6	How is access to the proprietary blockchain managed, by both the third party in control, and the business that uses the network?

5.1.10 Smart contract security assessment

Smart contracts are pieces of code that introduce business logic and capabilities to a blockchain system. How contracts are written, who is authorized to create them, and what happens when there are disputes are all important to understand when designing and assessing the quality and integrity of a blockchain system.

> **Smart contract security assessment control objective:** Smart contracts employed by the blockchain system are assessed for security and quality control prior to implementation and on a periodic basis.

The following risk assessment questions should be considered:

Smart Contract security assessment questions:	
1	Do existing or new smart contracts undergo a security review prior to implementation? • Does the implementation of a smart contract depend upon approval by someone with appropriate expertise in the implications of the security review results? Have the smart contracts in use undergone initial (and as applicable, periodic) security assessments? ● How are results of security assessments resolved, remediated, or addressed otherwise? ● Has the smart contract been approved by a person with appropriate expertise and authority? o Where has the approval been recorded?
2	Are there control mechanisms for upgrading or removing smart contracts from the chain? ● If yes, what are they? o Do they include addressing smart contracts that can no longer pass a security assessment?
3	Has the code of the smart contract been reviewed and/or tested prior to implementation, to determine if it will execute when and as intended?
4	How is smart contract operation monitored and reviewed? ● What is being monitored and reviewed? ● How often does the monitoring and review take place?
5	How are smart contract execution failures detected? ● If detected, what would be the process for recovery or fix?
6	If a defective smart contract executes or continues to execute, what risk would be created?

5.1.11 Inception and execution of smart contracts

Given the potential for smart contracts to automate legal and/or business processes, stakeholders should have proper controls in place to both deploy the smart contract and monitor its ongoing actions (if any). Unexpected behaviour and unanticipated consequences of smart contract execution can have significant consequences. A smart contract will execute as designed, but the design may be flawed or could be hacked. In these cases, upgrades are possible by designing new contracts to interact with the original contract, or a kill switch can be programmed into the code in some cases. However, these remedies can stop further damage, but other measures would be needed to address any problems caused by the flawed or hacked code. Thorough testing before inception and ongoing monitoring of execution is important to avoid additional risk.

Inception and execution of smart contracts control objective: Adequate audit trails exist to track the inception and execution of smart contracts.

The following risk assessment questions should be considered:

Inception and execution of smart contracts questions:	
1	What access restrictions exist for deploying smart contracts to the blockchain? How is the initiation of a smart contract logged?
2	Is there a time-lapse between initiation and execution of smart contract code? ● If there is a lapse, what risks, if any, could this introduce? ● How is execution confirmed?
3	Are provisions in place to address the failure of a smart contract to execute?
4	What data feeds into each smart contract to trigger its execution?
5	What data is written into the blockchain record because of the execution of the smart contract?
6	If a smart contract were to execute incorrectly or not as designed, what steps could be taken to recover? For example, if a bug such as the loophole discovered in the DAO ‘hack’ were to occur, fundamental principles of the system such as immutability, or agreements among participants may be challenged.

5.2 Governance and Operations

The maintenance of a blockchain by a network of participating nodes is structurally very different from traditional centralized database systems management, and as a result, requires specific consideration, processes, procedures, and governance. The ongoing operation of the chain includes a level of consensus about the state of the chain, its operation, the addition of data to the chain, and the potential for network splits (known as forks).

Governance and Operations include the following subsections:

- Consensus protocols
- Governance model
- Maintenance responsibilities
- Access management
- Jurisdictional laws, regulations and rules
- Standards
- Change management
- Managed services (hosted)
- Other external blockchain or other distributed networks (multi-chain)

Governance and Operations overall control objective: Governance regarding the management of the blockchain, including consensus protocols, maintenance requirements, member access, managed services, change control, applicable laws and other standards, has been defined and is adequate to ensure the integrity of the blockchain system and operations. This control objective should be considered in addition to control objectives in each Subsection below.

5.2.1 Consensus protocols

During the initial planning and development of the blockchain solution, the governance process is used to determine roles, responsibilities, and what determines consensus. Stakeholders may also want to understand and map the roles and hierarchies of authority (if applicable) among the nodes/connections in a particular implementation to understand the processes associated with consensus and approving the block to the chain.

> **Consensus protocols control objective**: Controls exist to ensure that consensus mechanisms are properly vetted, executed, and managed in accordance with participant agreements.

The following risk assessment questions should be considered:

Consensus protocols questions:	
1	How many nodes are required to: ● Reach consensus? What is the impact of the addition of a node? ● Provide sufficient resiliency? ● Incorporate agreed to security requirements?
2	How does the consensus process detect malicious behaviour by one or more nodes? ● If the behaviour is detected, what happens?
3	What monitoring is in place to manage external threats to the consensus process (e.g. ransomware attack)
4	How does the consensus process facilitate agreement between nodes?
5	If using a random election process for selecting validator nodes, how is randomness maintained?
6	How is a transaction finalized and how does this relate to transaction finality?
7	Are incentives used? If so, what are they? ● What purpose do those incentives serve? ● How are incentives earned? ● Can the incentives be taken away? ● How are incentives tracked and their distribution monitored? If some of these incentives are in the form of transaction fees, who pays the fee, when, and why?

5.2.2 Governance model

Decentralization, at least to some degree, is a key feature of blockchain design. In such a system, no single authority governs the state of that system (unless it has been designed to have a single authority in a private, permissioned context). Given this range of flexibility in governance model versus a traditional centralized database system where having a single authority is a given, stakeholders should understand how the specific governance model implemented functions for the blockchain being evaluated.

In the context of a blockchain, there are also roles that a third party may play which are not applicable to traditional database systems, such as a node in the network responsible for maintaining the chain. Given that blockchain technology is relatively new, stakeholders may wish to assess the expertise of any third-party service providers offering solutions or support for a blockchain system. Though other third parties beyond hosted services may be employed specific to a particular use case, such as crypto-asset custodial services, this technical report considers a use-case specific risk assessment out of scope.

Adequate due diligence over third-party providers and clear definitions of their roles and responsibilities in the blockchain system is required. Technology, and some of the service providers who create and service it, may be untested due to the relative newness of the technology itself, so stakeholders should use caution.

The choice to hire or train the in-house expertise to maintain systems versus using a service provider should involve risk and benefit analysis and may depend on the blockchain use case.

Vendors may be new to both blockchain and to business, introducing potentially new risks from those evaluated under legacy vendor assessment processes. Additionally, code from open-source projects is common in the blockchain space, as it is in other legacy technology, and can introduce additional risk as well as benefits.

> **Governance model control objective**: Governance is adequate to ensure that all parties can rely on the integrity and operation of the blockchain.

The following risk assessment questions should be considered:

Governance model questions:	
1	To what degree is governance automated? ● Is the automation achieved through smart contracts? ● If governance is not completely automated, what portions are excluded and how are they governed?
2	Does the governance model provide the level of flexibility needed to adjust to changing conditions? ● Is there a process to execute for policy exceptions?
3	Are off-chain models part of the governance? ● If off-chain is not part of the governance process, how are off-chain activities managed in conjunction with on-chain requirements?

Governance model questions:	
4	If blockchain is a backup for a legacy system? If so: ● How are they reconciled and kept in sync? ● How frequently does the backup occur?
5	How will changes to the governance model or to business rules be managed?
6	If the system is designed to operate without a single governance body, such that governance authority is distributed, how has the distribution of power been defined and assigned?
7	Could a governance decision split this blockchain (create a fork)? ● If a fork occurs, what governance process is in place to resolve or manage the fork?
8	How does the governance address cross-chain requirements/activities (if applicable)?
9	Does the governance process include data specific requirements such as: ● Data retention (type of data and duration of storage)? ● Data deletion/erasure while maintaining the integrity of the blockchain? ● Data subject rights for regulated financial and other data?
10	Does governance include or reference incident response processes?
11	Does governance include or reference recovery or resilience requirements if an event occurs?
12	Is there a formal Governance and Risk Management Program to perform due diligence and ongoing monitoring, and to identify risks associated with using third parties as service providers? ● What is the third-party vetting process? ○ How is the competence and expertise assessed? ○ Does the process address a third-party that is new to business and/or specific to the blockchain space? ○ Does the process include the identification of the role that open-source software plays in the third-party's support of the blockchain process? How will obligations be discharged? ○ Does the service provider carry cyber insurance? If so, does the cyber risk insurance policy include language specific to blockchain systems? ● Is the third party a node in the network?

Governance model questions:	
	○ If so, what are their responsibilities? ○ If not, what role do they play, and how do they access the network? ● If reliant on third-parties for knowledge, and expertise, what are the contingency plans to manage systems if the relationship must be terminated? ● What is the ongoing monitoring process for third-parties? ● Are risks identified and formally acknowledged? By whom? ● Are core responsibilities, service levels, and liabilities of all third parties documented and understood?

5.2.3 Maintenance responsibilities

As blockchain systems are distributed by nature, there will likely be multiple entities participating in the network to maintain the chain. Stakeholders should understand how these parties will cooperate on system management and maintenance issues and whether the multi-party nature of this maintenance poses any additional risks to the system overall.

> **Maintenance responsibilities control objective**: Maintenance responsibilities in a blockchain system are carried out under as defined by the governance, policies and procedures.

The following risk assessment questions should be considered:

Maintenance responsibilities questions:	
1	What is the release management process under the consortium framework for updates to code/applications, databases, operating systems, and infrastructure?
2	Who is responsible for overall updates - security patching; code updates; other changes?
3	What is the process for updates and how is it defined based on the type of update being applied (i.e. security patch releases)? ● Who performs and manages the updates?
5	Are the expectations for overall operations documented, such as service level agreements (SLAs) for maintaining and updating the environment?
6	How do the parties categorize low, medium, or high priority issues across the components of the blockchain environment?
7	Who monitors node traffic?

Maintenance responsibilities questions:	
	● Who is responsible for traffic spike notifications or anomaly reporting?
8	Who performs security assessments and how often are they performed?
9	How will all parties know reports are complete and accurate (i.e. addresses the multiple areas and processes within the blockchain)?

5.2.4 Access management

As in any database system, stakeholders will need to track system access and appropriate authorization procedures. Due to the reliance on cryptographic keys and digital signatures to maintain the integrity of the data in the ledger, stakeholders will want to pay close attention to the connection between these tools and the "real world" identity of the entity they represent.

> **Access management control objective**: Access management processes exist to ensure that members are authorized, and roles/entitlements are granted once approved.

The following risk assessment questions should be considered:

Identity and access management questions:	
1	How are changes to access levels and onboarding/offboarding managed?
2	What type of security is implemented (tokens, keys, certificates, other multi-factor solutions)?
3	Who has management or oversight of the security solutions (i.e. separation of duties)?
4	Do administrators have access to security components of users (e.g., tokens, keys, and so forth)?
5	Who provisions the access levels? ● If provisioning is automated, what monitoring, reporting, or alert mechanisms are in place?
6	What is the frequency with which access levels are reviewed? ● Who is responsible for the review?
7	Who is permitted to read data?
8	Who is permitted to write data?
9	Who is permitted to access specific nodes or enable node functions?
10	Where applicable, how is user screening for compliance with AML/CFT and sanctions laws and regulations supported?

5.2.5 Jurisdictional laws, regulations, and rules

With a traditional centralized database system, it is typically more clear what jurisdictional rules apply to the system and the data it manages. In a distributed blockchain system, the applicable rules may be less immediately clear, and all participants, including IT service providers, may need to understand which rules apply and when.

> **Jurisdictional laws, regulations and rules control objective**: Adequate controls are defined to ensure compliance with applicable rules and regulations within the context of the blockchain system.

The following risk assessment questions should be considered:

Jurisdictional laws, regulations and rules questions:	
1	What jurisdictions is the blockchain subject to, if any? ● If it is cross-jurisdictional, whose rules apply? ● What rules, if any, can be opted-out of?
2	Has compliance with AML/CFT, sanctions, and other similar rules been addressed?
3	How are the requirements of any new laws, regulations, and rules incorporated?
4	What is the communication plan for working with regulators and law enforcement to address misunderstandings or questions?
5	What are the jurisdictional issues for a service provider for IT compliance or adherence?
6	Is there a process to manage third-party service providers (due diligence, contracts, roles and responsibilities, monitoring, annual review)? (See also Governance model section **5.2.2** and Maintenance responsibilities section **5.2.3**)
7	Are all service providers operating in the same jurisdiction? ● If operating as a service provider for customers in the same jurisdiction, what are the results of the jurisdictional analysis assessments?
9	Are any clients or providers listed on or located in a sanctioned jurisdiction that would compromise the organization, operation, or transactions of the blockchain (e.g., OFAC list)?
10	What are the terms and conditions for use of different products and services and are there variations by jurisdiction?

5.2.6 Standards

Like any other software system, a blockchain and its constituent components should adhere to applicable national and international technical standards developed for financial information systems for the system design, security, and maintenance. Refer to References, section 2, for a list of standards and other documents that may be applicable to certain blockchain use cases and architectures. Adhering to accepted standards supports the security and efficiency of the system.

> **Standards control objective**: Internal controls exist to ensure applicable national and international technical standards developed for financial information systems are applied to system design, security, and maintenance of the blockchain system.

The following risk assessment questions should be considered:

Standards questions:	
1	What framework is being used for the controls and security of the blockchain platform – e.g. NIST, ISO 2700x, CIS, ISF, or other security framework?
2	Are all major and minor software components and corresponding systems/infrastructure approved for use within the organization?
3	Are third parties that are part of the environment assessed through a formal and detailed process that includes due diligence and compatibility of the third-party?
4	How are new standards addressed? ● Is a process for adherence needed?
5	Is the design of the system flexible enough to address new or emerging standards?
6	What is the risk if standards and processes have not been formalized?

5.2.7 Change management

Since a blockchain environment consists of multiple components from application code to the underlying systems and platform supporting the solution, a formal change management process needs to be designed, implemented and adhered to. Procedures and processes to include appropriate communication, documentation and testing should consider the distributed nature of blockchain systems. When a change is made within one organization that may affect the collective network, appropriate steps should be taken to notify and address any concerns that may arise.

> **Change management control objective**: Controls exist to any change introduced to the blockchain systems to ensure the change is authorized, tested, approved and verified by appropriate parties prior to changes being implemented.

The following risk assessment questions should be considered:

Change management questions:	
1	How are updates or necessary changes determined, defined, and documented?
2	Who has been assigned responsibility for the updates?

Change management questions:	
3	If multiple parties are part of the update process, how is coordination of updates occurring?
4	How will updates of the following, as well as any other updates be deployed? • Application/code changes • Bug fixes • Security patches • Platform changes
5	How are changes tested and further revised as needed?
6	How are changes authorized?
7	What are the detection mechanisms for unauthorized changes?
8	Has backwards compatibility been tested?
9	How is cross-version (cross-chain) compatibility maintained? Can nodes and/or end-user clients safely use different versions of the software to interact with the blockchain?
10	Is there a versioning process for the software?

5.2.8 Managed services (hosted)

As in traditional database systems, components of a system that are managed by service providers mean that those providers' own cybersecurity risks will be indirectly borne by their clients. These concerns are similarly relevant in the context of a private, permissioned blockchain, particularly if the entire platform is being offered in a "blockchain-as-a-service" model. For example, a managed service may support the network, operating, and communication and data management system layers, providing application programming interface (API) connections for proprietary development of the application layer and implementation of business rules. As such, stakeholders should know specifically what responsibilities lie with the managed service provider and which are the purview of the business and its development team.

> **Managed services (hosted) control objective**: Controls existing to ensure that the scope roles, responsibilities, and actions of all managed service providers documented and monitored.

The following risk assessment questions should be considered:

Managed services questions:	
1	What part of the code does a hosting service control? ● Who controls the application logic and/or business rules? ● How do updates to lower-level code impact customized development at the application level? ○ If code changes are needed, what are the communication responsibilities of each party? ○ What compatibility testing is needed when changes are implemented?
2	Will information on security be shared at the level needed?
3	Are managed services using open-source software? ● If used, what is the provider's practice when using open-source code?

5.2.9 Other external blockchain or other distributed networks (multichain)

Much like the internet itself, blockchain systems may operate as a patchwork of networks. For example, one blockchain network might exist to store transaction records, while another blockchain network might be used to perform the transactions themselves, including the movement of funds. If a variety of blockchain networks are used to provide a solution, it is important to understand how these networks are used, where authority lies, and how data is exchanged between networks, if at all.

There could be a need to connect or interface with external blockchain or distributed ledger networks. Ensuring compatibility / interoperability will be critical for accurate and timely processing of transactions. Interfacing with external systems could present security and operational risks but may be necessary to ensure access and overall system resiliency.

> **Other external blockchain or other distributed ledger networks (multichain) control objective** Controls existing to ensure that the scope roles, responsibilities, and actions of multichain networks are documented and monitored.

The following risk assessment questions should be considered:

Other external blockchain or other distributed networks (multichain) questions:	
1	How are the external blockchain or other networks connected? ● What is the purpose of the other network?
2	How is the data exchanged?

5.3 Trust and Resilience

Neither cryptography, nor hash functions, are unique to blockchain. However, blockchain's heavy reliance on these technologies to deliver on the 'trust' expectations within a multi-party ecosystem could be considered unique to blockchain. Therefore, stakeholders may want to pay added attention to these elements when evaluating the risks of a blockchain system.

As computing capabilities strengthen, cryptographic algorithms should also continue to evolve to maintain the required security. Cryptographic systems should be evaluated for agility—how quickly can migration and update occur—to support necessary change. In addition, certain flaws inherent in the algorithm become apparent over time and use, which further deprecates their utility and security ages as computing resources increase or new methods are devised. This algorithm aging process should be anticipated in DLT systems design. Cryptographic protection of long-lived data should be managed to ensure against loss of integrity and authenticity and non-repudiation. This management may require the encapsulation of signed data using signatures that rely on stronger algorithms. The confidentiality of cryptographic keys used to safeguard information should be preserved, and the keys should remain available for use.

Trust and Resilience contains the following subsections:

- Cryptographic algorithms
- Public key infrastructures
- Resilience, data persistence and continuity of operations
- Identity management

Trust and Resilience overall control objective: Reasonable care has been taken to ensure that the cryptographic tools used in each blockchain system are appropriate for its use and applied in a way that engenders overall trust in its integrity and recovery. This control objective should be considered in addition to control objectives in each Subsection below.

5.3.1 Cryptographic algorithms

DLT systems may use cryptographic algorithms to provide data confidentiality and privacy, integrity, identity authentication, origin authenticity, and non-repudiation services. Security, privacy, and confidentiality guarantees are based on the strength of the underlying cryptographic algorithms.

Cryptographic hash algorithms are used to provide data integrity and authentication. DLT data needs to be preserved for a long time to provide provenance while the cryptographic algorithms deployed to protect the data may need to be replaced over time to counter the constant attacks. That conflicting dynamic of data longevity and the need for flexibility in the architecture to accommodate algorithmic maintenance and change, referred to as "crypto-agility," is one of the biggest challenges of DLT. With the advances in quantum computing and their predicted ability of compromising current security-based algorithms, the use of quantum safe algorithms becomes a more pressing issue.

For a detailed discussion of applications of the cryptographic algorithms in DLT, please refer to Annex C.

Cryptographic algorithms control objective: Cryptography and key management comply with the security policies of the organization and appropriate X9, NIST, and ISO TC68 standards.

The following risk assessment questions should be considered:

Cryptographic algorithm questions:	
1	Which cryptographic algorithms support each of the following functions: ● Entity identification? ● Entity authentication/ Origin authentication? i.e., Who signed this? ● Data integrity? ● Data confidentiality/privacy?
2	Is there evidence that use of cryptographic algorithms is documented and disseminated to all stakeholders?
3	Are the cryptographic algorithms used approved by appropriate standards organizations, (e.g., X9, ISO, NIST)?
4	Who (or what entity) is responsible for managing the algorithms and handling keys? ● Do the cryptographic algorithms and protocols used comply with the policies of each organization participating in the system?
5	Is encryption or tokenization used to protect data? What data is protected by encryption or tokenization?
6	What key management standards, techniques, and controls protect the cryptographic keys?
7	What are the encryption strength requirements?
8	What assurance is available to demonstrate that the encryption meets these strength requirements?
9	If the system utilizes hash functions, what hashing algorithm is used? ● Is the algorithm commercially/publicly available, or proprietary?
10	To what extent does the security of the blockchain system overall depend on the security of the hash function(s) used? For example, if an attacker has ‘data’ and the hash (‘data’) then they can alter the ‘data’ and compute a new hash without a key and without detection, unless the hash is protected by a signature.
11	Does the system support the ability to move from the use of one algorithm to another when the need arises? ● Is the cryptography in the system modular such that it could be swapped out if a vulnerability were found in a particular algorithm? ● Or is it embedded in an inextricable way such that a change or compromise would endanger the accessibility of the on-chain data, or loss of compatibility between an on-chain reference and an off-chain asset? ● If the algorithm changes, how are the older blocks affected?
12	Have standards from recognized standards bodies (e.g. ISO, X9, NIST, etc.) been applied where appropriate?

Cryptographic algorithm questions:	
13	Is there a documented Key Management Lifecycle (KML) policy for the system?
14	How are the lifecycles of certificate-based keys managed in areas such as digital signatures, key management, Cryptographic Message Syntax, etc..?
15	How long are signature verification keys retained?
16	How are algorithm requirements enforced in the system?
17	Are there procedures in place for managing the risks to long term data of signature algorithms, key sizes, and domain parameters becoming obsolete or subject to attack?
18	Are multiple cryptographic algorithms supported?

5.3.2 Public key infrastructures

Blockchains, and more generally DLT systems, typically rely on public key infrastructures for access management and other functions. As such, though public key infrastructure management and risk assessment is not new to blockchain, the importance of these infrastructures may be heightened given the critical role they play. See Annex B for more information on public key infrastructures.

> **Public key infrastructure control objective**: Public key infrastructures and certificate management technologies, practices, and procedures should comply with X9 and ISO TC68 standards

The following risk assessment questions should be considered:

Public key infrastructure questions:	
1	Does the blockchain rely on public key infrastructure for: ● Entity identification? ● Entity authentication? ● Data integrity? ● Data confidentiality/privacy?
2	Does the public key infrastructure comply with X9/ISO TC68 standards
3	Do certificate management policies and practices comply with X9/TC68 standards
4	What is the key management model?
5	Are copies of private keys allowed? ● If so, how are they managed/protected?
6	Is there a registration process?
7	How are keys related to users?
8	How is access related to keys and users?
9	Is there a recovery process for lost keys?
10	Is there a process for deactivating or flagging stolen keys?
11	Is there a certificate authority?
12	Is there a plan for mitigating exposures due to quantum computing risks i.e. post-quantum cryptography? For example, are group or ring signatures allowed?[4]
13	How is certificate revocation of multiple CAs communicated to stakeholders?

5.3.3 Resilience, data persistence, and continuity of operations

Traditional databases may rely on replication and standardized failover systems to achieve resilience and meet business continuity targets. Blockchain systems, via distributed nodes that collectively maintain the state of the system, are intended to be more resilient than a standalone database instance by design; however, in a private, permissioned context, stakeholders may wish to investigate this assumption more completely. For example, the

[4] See Informative Annex A Group Signatures

number of nodes considered sufficiently resilient based on the use case and expected performance of the system may vary.

Resilience, data persistence and continuity of operations control objective: Internal controls exist to ensure the continuity of operations of the blockchain system.

The following risk assessment questions should be considered:

Resilience, data persistence, and continuity of operations questions:	
1	Is there an external backup, such as in a traditional database or other system, for the information on the chain?
2	If the only backup of the ledger is the copies maintained by participating nodes, how many nodes are needed to meet resiliency requirements?
3	Is the design of the system able to meet resiliency/recovery time requirements?
4	What are the mitigation practices or alternative options if the system fails?
5	What are the testing plans?
6	Has failover testing been performed for any backup systems?
7	What continuity testing or business recovery tests have been performed?
8	How is the system health monitored?
9	Is there a documented Disaster Recovery (DR) / Business Continuity (BC) Program for the system? ● Is there a clear line of responsibility assigned for maintaining the DR/BC documentation? ● Does the responsible party have funding resources necessary to perform their duties? ● Are DR/BC procedures regularly and periodically tested? ● Does DR/BC testing include moving back from recovery sites to normal operations? ● Are the results of periodic DR/BC testing documented and used to improve the DR/BC procedures? ● How are cryptographic materials managed in preparation for and during DR/BC events?

5.3.4 Identity management

For permissioned blockchain systems used within financial services, managing the identity of participating nodes or connected systems is important. Particularly when a blockchain system is meant as a message or value exchange among a consortium of entities participating in a common purpose, understanding the identity of each participant supports the overall security of the system and the operation and governance policies established by the stakeholders.

Vetting the identity of a participant in a DLT system requires examination by a trusted registration authority (RA). The vetting process should meet the documented policy requirements for enrolment in the system. The RA should ensure the validity and suitability of the proof of identity provided by an entity before enrolling the participant and issuing the participant an identity authentication credential.

Once enrolled, an identity authentication credential can be used by the participant to gain access to the system. The access control system should verify that the credential presented by a user in an attempt at authentication is valid. This process should provide assurance that the credential can be traced back to the registration authority process that vetted the user identity at the time of enrolment in the system.

For a PKI-based authentication system, this identity tracing requires that the access control system perform certificate path validation from the presented user credential back to the trusted root or trust anchor of a certificate issuing authority. For a password-based system, this tracing requires ensuring the credential is associated with the system account of the user whose identity was vetted by a registration authority when the user account was authorized.

> **Identity management control objective**: Identity management technologies, practices, and procedures should comply with X9 and ISO TC68 standards.

The following risk assessment questions should be considered:

Identity management questions:	
1	Does the blockchain rely on an identity management system?
2	How are the following entities in the blockchain system and their owners identified? ● Nodes ● End-users ● Processes ● Smart contracts ● Validators
3	Do identity management technologies, policies and procedures comply with X9/TC68 standards?
4	Are identities tied to a Public Key Infrastructure (PKI), Zero Knowledge Proof (ZKP) or some other mechanism?
5	Are role-based access control (RBAC) or attribute based access control (ABAC) mechanisms used? ● If provisioning is automated, what monitoring, reporting, or alert mechanisms are in place?
6	How is the privacy of users achieved?

5.4 System Integrations

Most blockchain systems will rely on inputs from legacy or new systems and these integration points will warrant attention. Additional systems and tools provide or enable inputs or will receive output to enable a particular use case. Integrations between traditional databases or multiple blockchain systems may be likely. The following sections highlight integration points stakeholders may want to review to understand risk and assess where emergent conditions arising from new integration points could lead to the need for additional controls or caution.

System Integrations includes the following subsections:

- APIs
- Interoperability
- External data sources (oracles)

System Integrations overall control objective: Connections with external systems should be secure and resilient to failures. Responsibility for failure should be articulated. This control objective should be considered in addition to control objectives in each Subsection below.

5.4.1 APIs

Traditional systems integration issues will continue to apply to blockchain systems. APIs may be used to simplify interactions with the blockchain by leveraging a host of communication protocols and tools that can be used to build additional applications on top of the existing functionality.

APIs control objective: Internal controls exist to ensure APIs are defined, documented, and subject to change management processes.

The following risk assessment questions should be considered:

APIs questions:	
1	Is there an API between the blockchain and other systems interacting with it? • If a legacy system is incompatible with the blockchain system and an API is needed, what is the API doing and how is it secured? • If integration breaks between any two or more systems, how is the failure detected and who is liable? • Who manages the API, including making any updates and providing technical support on an ongoing basis? o How is it protected from unauthorized modification?

5.4.2 Interoperability

A blockchain may need to share or access information across different networks to meet business needs. By interoperating with external networks, a blockchain can connect with both legacy systems and other blockchains to incorporate different data sources, reach higher throughput, increase redundancy, or enhance security.

Interoperability control objective: Internal controls exist to ensure that interoperability is maintained according to the design and architectural principles of the system

The following risk assessment questions should be considered:

Interoperability questions:	
1	How does the blockchains interact with external systems? • What are the entrance and exit points? • How regularly does information accessed from external systems get recorded on the blockchain?
2	How are reconciliations of blockchain ledgers with traditional general ledger systems performed?
3	Do any external system controls affect the accuracy of data on the chain? • If a flaw in an external system pollutes the blockchain data, what are the integrity checks?
4	Do external systems follow the same access control procedures as the blockchain system? • If not, why are they different?
5	If two or more blockchains are interacting, how does reconciliation of cross-chain transactions occur?
6	Does the blockchain interact with or rely on other external systems to meet business needs?
7	What specific businesses cases rely on other networks relaying information to the blockchain**?**

5.4.3 External data sources (oracles)

A blockchain may receive information from external data sources to meet business needs. These external data sources may not be subject to the underlying blockchain's security mechanisms and should be assessed separately to understand where risks may lie. These external data sources may be referred to as oracles.

> **External Data Sources (oracles) control objective**: Internal controls exist to ensure the blockchain has adequate controls that provide reasonable assurance over the integrity of external data sources.

The following risk assessment questions should be considered:

Oracle questions:	
1	What is the purpose of the oracle in the operation of the blockchain under review? ● What specifically does the blockchain rely on the oracle to do? ● What specific data is the oracle relaying to the blockchain? ● How is the authenticity and integrity of oracle data provided? ● Is oracle data confidentiality required, and if so, how is confidentiality achieved?
2	What set of controls are in place? ● What IT and business internal controls are in place to govern the use of data from an oracle? ● What IT and business controls exist over how the system is updated and maintained? What IT and business controls are in place to ensure the availability and reliability of the system?
3	How frequently does the system send information to the blockchain?
4	If the system is unavailable, what is the impact on the operation of the blockchain?
5	Are there any contingencies in place in case the system either fails to relay or relays bad information to the blockchain?
6	Does the oracle operate in a decentralized environment, or rely on a central operator to ensure data is relayed to the blockchain?

5.5 Smart Contracts: Legal and Business Processes

Smart contracts are often the mechanism for executing automated activities on a blockchain. They are “triggered” by certain conditions and “run” according to certain rules specified in their computer coding. Though if/then code executions are not new, the intended finality of transactions executed autonomously by smart contracts are a novel component of blockchain-based systems.

Smart contracts are the expression of an agreement encoded on a blockchain, but enforcement of the contract itself is a legal action. Because a smart contract will execute as written, stakeholders should establish clear agreements up front and have dispute resolution procedures ready to address issues. Assessments of smart contracts in a blockchain system might need to evaluate both whether the contract executes as designed, and whether the execution of the action conforms to the intent of the agreement. The following sections provide questions for stakeholders including auditors and others responsible for the integrity and operations of the blockchain to ask about how smart contracts work and whether they execute appropriately.

Smart contracts allow for the automated performance of legal or business processes and the execution of obligations undertaken by parties to a legally binding contract. Stakeholders should ensure that smart contracts used for such purposes have the legal effect and business outcomes intended.

Smart Contracts: Legal and Business Processes overall control objective; Controls should exist such that Smart Contracts that are executed on the blockchain, or are executed by another smart contract or transaction on other system are properly documented, are maintained, and have a reliable audit trail. This control objective should be considered in addition to control objectives in each Subsection below.

The following risk assessment questions should be considered:

Smart Contracts: Legal and Business Processes questions:	
1	Is the intent of the parties to a legal contract underlying the smart contract and the expected outcome of the execution of the smart contract documented in some form? Consider: ● What is the inventory and accounting process for all smart contracts of the blockchain solution? ● How is the function of each smart contract documented? ● What testing demonstrates that the executable code of a smart contract performs as intended? ● What methods are used to account for the execution of a smart contract (e.g., transaction triggers, version control, certificate authority, date/time)? ● How are users of the blockchain solution assured that functions are in fact executed by the smart contract?
2	What IT and business controls ensure that: ● Amendments to an underlying legal contract are also accurately made (as applicable) to the code of the smart contract? ● Changes to the code of the smart contract are properly reflected (as applicable) in the underlying legal contract through amendment?
3	How are potential changes to the code of a smart contract integrated into a formal change management process? ● What testing and change management processes are used for smart contracts? ● Are unique procedures used for different classes of smart contracts (e.g., generic, utility, industry use case)?
4	Who has the authority to develop, test, and implement smart contracts and changes to smart contracts?
5	If performance of a critical business activity depends on a smart contract, what plans are in place to correct for errors in its execution? ● Is the consensus mechanism being relied upon to resolve disputed outcomes that result from execution of a smart contract? ● Are other dispute resolution procedures in place?

Smart Contracts: Legal and Business Processes questions:	
6	Is an event that triggers the execution of a smart contract ever validated against reality? ● If so, what is the method and process of verification? For instance, a smart contract may be programmed to initiate a payment to an exporter when the importer takes possession of the goods. When a sensor aboard a ship notes that the ship has stopped moving and that the weight of the cargo in the hold is zero, that alert triggers the smart contract to initiate a payment to the exporter. Are the sensor's readings ever validated for accuracy? Is the alert ever traced back to the source sensor to ensure that the smart contract is acting on an alert produced by the sensor on the correct ship?
7	Are outcomes as recorded on the blockchain by a smart contract ever validated against events off the blockchain? ● If so, what is the method and process of verification? For instance, parties may expect a smart contract to initiate a USD payment from Person A to another Person B, and record that initiation on the blockchain, after certain conditions are met. Is the recorded initiation ever validated against the payment instruction produced by the smart contract as received by Person A's bank?
8	Is information or data that is tied to a natural person being recorded on the blockchain? Does the blockchain comply with privacy regulations as they pertain to the use and storage of such information or data?
9	Who is the arbiter if the participants do not agree on the result of the smart contract's execution? ● How is dispute resolution documented?
10	● What business and IT controls exist to ensure transactions executed by smart contracts are reliable and conducted properly so that they may be enforced in a court of law if there is a dispute?
11	How does the consensus governance process ensure that parties engaged in a transaction using the blockchain solution specify that the blockchain is the system of record for the transaction?

Annex A
(Informative)
Group Signatures

Group signatures used in a private or permissioned blockchain can be associated with a certificate in a PKI. Typically, a public key certificate identifies the owner of only one private signing key. In a group signature scheme, a single public key certificate is shared by a set of group members. This serves to mask group member identities, providing them with a shared alias identity during signature validation.

A group signature provides data integrity and origin authenticity along with some degree of privacy for the signer. In a group signature scheme, each group member has their own private signing key. All group members share a common public key. This single public key can be used to verify the signature of any group member.

The degree of privacy afforded to group members depends on several factors, including the size of the group. However, group signers are not anonymous. It is possible for a financial services organization to comply with AML/CFT requirements while operating a group signature scheme. A group signature policy should be used to manage the risk of noncompliance with the organizations legal and regulatory requirements.

Group signature implementations require a group manager, a central authority who can open any group signature to reveal the identity of the signer. This makes group signature schemes useful in systems that need to detect or prevent double-spend. In some group schemes, it is also possible for a group manager to link signatures created by a particular signer.

As with all PKI certificates, a group certificate can be revoked. Group certificate revocation ends the ability to verify signatures of the entire group. Some schemes offer more granular revocation, making it possible to revoke a single member, or to restrict the scope of what a given member may sign.

Audit considerations for group signature schemes should include the control objectives that apply to a traditional PKI. A specific policy describing group signatures should exist. The practices associated with this policy should be documented in a certificate subscribers SLA. This documentation should detail what features are available in the group signature scheme, and how such features as signature opening, linking, and revocation are operationally supported.

Annex B
(Informative)
Public Key Infrastructures

Designers of DLT systems that rely on a Public Key Infrastructure (PKI) should be prepared to manage transitions between Certificate Authority (CA) public keys. These transitions are referred to as “key rollovers”. These transitions can be well-planned and coordinated to prevent disruptions to the system, or they can be uncontrolled, occurring at any time without warning.

Public Key Infrastructures are important for establishing trust and conforming to security protocols in DLT systems. The certificate authority (CA) of the PKI in the DLT system has the right to create and issue certificates to authorized requesters. Issued and accepted certificates are marked as valid through publication to a certificate repository, another entity which keeps records of valid certificates with attributes like validity period and owner.

Public key infrastructure relies on asymmetric cryptography. Asymmetric cryptographic key pairs have two components: a public key that can be widely shared, and a private key that must be protected. When the confidentiality of private keys is compromised, data protected by digital signatures can suffer loss of integrity. When private keys associated with public key certificates tied to a PKI are compromised, assurance in the identity and authenticity of the signer may be lost, and it may be possible for previously signed transactions to be repudiated.

X.509 certificate management, is the PKI activity of monitoring, facilitating, and executing every certificate process necessary for uninterrupted operations of a DLT network. It is the process of requesting, deploying, renewing, and replacing certificates on their respective DLT endpoints (which could be an application, a server, a device – or any other network component). DLT certificate management should, possess functionality to monitor the entire certificate infrastructure in real time, and automate any certificate operation.

Annex C
(Informative)
Cryptographic Algorithms

DLT systems may use cryptographic algorithms to provide data integrity, identity authentication, origin authenticity, and non-repudiation services. To interoperate at a given point in time, participants in a DLT system should support a common set of cryptographic algorithms. Over time, the set of supported algorithms may change.

Cryptographic hash algorithms are used to provide data integrity in DLT systems. These hashes may be digitally signed to allow tampering of hashed data to be detected. When these signatures are tied to certificates in a Public Key Infrastructure (PKI), origin authenticity services are provided, allowing signer identification, and making non-repudiation possible.

Changes made to the cryptography used within the system may be well-planned and orchestrated to minimize disruption as participants migrate from one set of algorithms to another. Changes may also be uncontrolled and occur at any time. These disruptive migrations may be forced on participants by the development of new attacks on the algorithms in use, key compromise events, or performance increases in computation that effectively weaken cryptographic protections.

DLT system design should consider the need for cryptographic algorithm agility. In an agile design, it should be possible for the users of a DLT system to easily migrate to new algorithms over time. The DLT design should also anticipate forced migrations due to unpredictable changes in cryptography.

A documented policy for cryptographic migration within the DLT system should be defined. This policy should be communicated to all participants. The policy should become part of the participants disaster recovery (DR) and business continuity planning (BCP) procedures. These procedures should become part of periodic, continuing exercises that allow the procedures to be practiced and improved.

It should be possible for all participants in the system to identify the cryptographic algorithms needed to verify the validity of past transactions. For long-lived data, transactions may reside in the system for an extended period. To verify a digital signature to ensure the integrity and authenticity of the hashed data in a DLT system, the hash and signature algorithms and any associated parameters used by the signer must be identified and known.

A common practice for algorithm identification is to package cryptographic keys along with an algorithm identifier. Digital signatures and keys packaged in PKI certificates illustrate this practice. Other means of algorithm identification are also possible. Mechanisms may include using a transaction or block header to convey the algorithms currently in use, or to identify a point of algorithm set transition.

Bibliography

[1] ISO 10202 (All Parts) Financial transaction cards — Security architecture of financial transaction systems using integrated circuit card

[2] ISO 13491-1:2016 Financial services — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods

[3] ISO/IEC 7810:2019 Identification cards — Physical characteristics

[4] ISO/IEC 7813:2006 Information technology — Identification cards — Financial transaction cards

[5] ISO/IEC 7816 Identification cards — Integrated circuit cards

[6] ISO/IEC 9594-8:2017 Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks

[7] ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

[8] ISO/IEC 18032:2020 Information technology — Security techniques — Prime number generation

[9] ISO/IEC 18033 :2015 Information technology — Security techniques — Encryption algorithms — Part 1: General

[10] ISO/IEC 19790:2012 Information technology — Security techniques — Security requirements for cryptographic modules

[11] ISO/IEC 24759:2014 Information technology — Security techniques — Test requirements for cryptographic modules

[12] NIST FIPS 140-3:2019 Security Requirements for Cryptographic Modules