ISACA | AICPA & CIMA

Blockchain Risk

Considerations for Professionals

Emerging Technology

CONTENTS

ABSTRACT

Blockchain technology presents unique risk and benefits that must be weighed on a case-by-case basis. To help identify and assess blockchain risk, ISACA® and AICPA® & CIMA® formed a joint working group to focus on blockchain technology and risk in the context of business application.

In this white paper, the ISACA-AICPA & CIMA Joint Blockchain Working Group assigns blockchain risk to five domains:

- Governance
- Infrastructure
- Data
- Key management
- Smart contracts

Across these domains, the working group identifies a range of risk items and further:

- Categorizes each risk by domain and (if applicable) subdomain
- Assigns an identification number
- Names and describes the risk

Introduction

As more enterprises research, test and enable blockchain technology to advance business, operational, regulatory and strategic initiatives, management should understand that blockchain technology—like all technologies—comes with unique risk and benefits that must be weighed on a case-by-case basis.

Blockchain offers potentially transformational benefits—e.g., decentralization, immutability and finality—however, it is still a nascent technology and by no means one size fits all. A given implementation of blockchain technology may advance goals in one entity and yet impair those of another. Numerous types of blockchains—each with an array of options —confront any enterprise or entity hoping to determine the configuration that best serves its purposes.

Each type of blockchain poses its own risk, and should be evaluated carefully before implementation. For example, governance risk in a private (permissioned) blockchain differs considerably from governance risk in a public (permissionless) blockchain.

In a permissioned blockchain, management oversight determines and monitors who can participate, and what access to grant—while in a permissionless blockchain, access is open to anyone who wants to participate. Governance risk in a permissionless blockchain may include an element of privacy risk that does not arise with permissioned blockchains.[1] Specialized skills may be required to evaluate a blockchain and identify its unique risk based on facts and circumstances.

ISACA-AICPA & CIMA Joint Blockchain Working Group

To help enterprises evaluate and implement blockchain technology, ISACA and AICPA & CIMA formed the ISACA-AICPA & CIMA Joint Blockchain Working Group, with a core mission of identifying and documenting risk associated with blockchain technology. The group includes subject matter experts with a broad range of experience—from helping clients implement the technology to working with entities currently using it.

Scope and Focus of the Working Group

The ISACA-AICPA & CIMA Joint Blockchain Working Group is tasked to identify risk specific to private blockchains. Accordingly, this white paper focuses on private blockchains (although certain identified risk relates equally to public and hybrid blockchains).

[1] Privacy risk is outside the scope of this publication.

This white paper treats legal risk at a high conceptual level.[2] Generally, blockchain technology should be considered from the following legal vantage points:

- Blockchain technology—even though it is pseudo-anonymous —does not free an entity from the application of legal requirements that are otherwise standard.
- A blockchain can provide regulators and law enforcement agencies with an enhanced ability to trace transactions.
- Because information on a blockchain generally cannot be modified, regulatory or jurisdictional changes may potentially render a blockchain illegal or noncompliant with those regulations or jurisdictions.
- An implementation of a solution using blockchain technology may not act as a legally binding contract and/or qualify as a legally obligated record (i.e., for audit purposes).
- Blockchain immutability and/or storage on multiple nodes may conflict with privacy laws and regulations, e.g., the right to be forgotten under the General Data Protection Regulation (GDPR).
- Entities must consider laws, rules and regulations of the United States and its jurisdictions and territories, and other applicable jurisdictions outside the United States.
- Laws, rules and regulations applicable to the implementation of blockchain technology, e.g., in the financial services sector, typically are high level and broadly stated. Therefore, the spirit of the laws, rules and regulations should be considered.
- Any enterprise considering blockchain technology is advised to consult legal counsel.

Understanding Blockchain Risk

A wide range of practitioners should understand the risk surrounding blockchain implementation and operation, including:

- **CPAs**—To assist with identifying relevant risk in engagements
- **IT auditors**—To assess and monitor internal control over technology
- **Cybersecurity practitioners**—To evolve, manage and monitor security controls over information and technology
- **Management**—To understand potential risk relating to coordination and management of enterprise resources
- **Internal audit**—To understand risk with respect to enterprise internal controls, including corporate governance and accounting processes
- **Blockchain developers**—To heighten awareness of and mitigate potential risk in the development and optimization of blockchain protocols, crafting of blockchain architectures, formulation of smart contracts, and application of blockchain technology for other uses

Blockchain Risk Domains and Descriptions

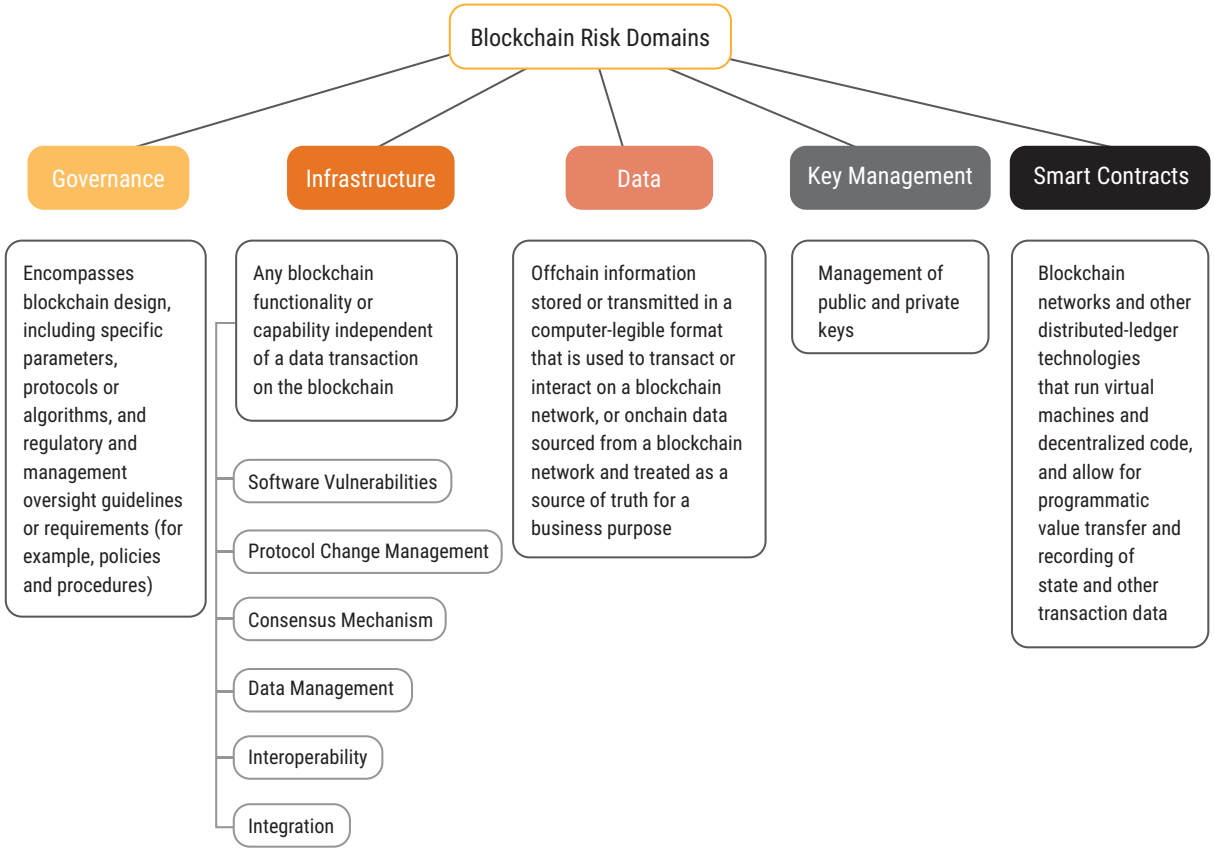
The working group identifies and categorizes blockchain technology risk across five domains (**figure 1**).

To elaborate blockchain risk domains, the working group:

- Assigns a risk identification number (R#) specific to each domain and subdomain e.g., 2.05 Interoperability
- Assigns a label, i.e., brief name of the risk
- Describes each risk and, where necessary, defines technical terms

[2] A full legal analysis is beyond the scope of this paper. Neither ISACA nor AICPA & CIMA should be construed to offer such legal advice.

FIGURE 1: Blockchain Risk Domains



The following table documents blockchain technology risk as it applies to all types of entities, organized by domain and unique risk ID.[3] Certain risk may persist across domains. Descriptions feature explanations of identified risk and its context, including vulnerabilities, exploits, attack vectors, improper configuration and management, etc.

Blockchain Technology Risk by Domain

Risk Domain and Subdomain	Risk Description
R-1 Governance 1.01 Design 1.02 Policies and Procedures	Encompasses blockchain design, including specific parameters, protocols or algorithms, and regulatory and management oversight guidelines or requirements (for example, policies and procedures)
R-1.01 Design	Design of the blockchain governance includes the specific model, parameters, protocols and algorithms.
R.GOVERNANCE.1.01.001 Baseline Deviation	Deviation from the approved baseline design (specific parameters, agreed-upon processes and protocol structures) compromises the protocol or system integrity.
R.GOVERNANCE.1.01.002 User Authentication/Password Parameters	Insufficient authentication configuration parameters may fail to address threats to the blockchain. For example, a system may be compromised due to brute force methods to crack weak or overused passwords, especially if there is no lockout procedure.
R.GOVERNANCE.1.01.003 Super/God Node/User Concept	An insufficient consensus mechanism (one that is not strong enough to deter all protocol or smart contract code changes) can create a centralized power (a super node) that is able to negatively impact the protocol or design of the system, causing it to fail.

[3] This table is intended to be broad and comprehensive, although not exhaustive and all-inclusive. Blockchain technology risk is not universal and varies according to local facts and circumstance. The table assumes that professionals have attained an advanced understanding of blockchain technology and strongly grasp its processes. For more general information on blockchain technology, see Appendix A: ISACA and AICPA & CIMA Blockchain Resources.

Risk Domain and Subdomain	Risk Description
R.GOVERNANCE.1.01.004 Unconfirmed Transactions/Processes	Lack of protocols for unconfirmed transactions can allow processing of fraudulent transactions that were previously rejected, thereby posing a threat to the network.
R.GOVERNANCE.1.01.005 Preventing or Limiting Forks	Baseline design errors may enable nonvalid soft or hard forking on the network, subjecting transactions and network assets to risk of loss.
R.GOVERNANCE.1.01.006 Jurisdictional or Regulatory Changes	Future jurisdictional or regulatory changes may render a particular blockchain solution illegal or noncompliant, or otherwise require a fundamental change to the blockchain structure, function and governance model.
R.GOVERNANCE.1.01.007 Block Creation	Insufficient protocols for block creation, e.g., size of block and frequency of blocks being added, can lead to failure of the network system.
R-1.02 Policies and Procedures	The governance policies and procedures include regulatory and management oversight guidelines or requirements of the blockchain.
R.GOVERNANCE.1.02.001 Minimum Access Policy	Participants with more access than necessary to perform their function can lead to intentional or unintentional damage to the system.
R.GOVERNANCE.1.02.002 Incident Response Plan (IRP)	Lack of an adequate plan to respond, mitigate and recover from a detected compromise may result in damage or liability.
R.GOVERNANCE.1.02.003 Node Checks for Rogue Nodes/Users	Improper policies to protect the network from rogue or unauthorized nodes can damage or compromise the network. For example, inactive users should not be able to view or access any transactions.
R.GOVERNANCE.1.02.004 Compromise of Validating Nodes	Lack of monitoring the consensus can lead to compromised validating nodes, which can result in the blockchain reaching an inappropriate consensus or being unable to reach consensus.
R.GOVERNANCE.1.02.005 Identity of Participants	Lack of know-your-customer (KYC) policies to determine the identity of a participant can mask other policy violations (e.g., a conflict-of-interest policy that applies to a vendor on a private supply chain who is also employed by the buyer) or illegal activities, resulting in compromise to the trust and integrity of the blockchain.
R.GOVERNANCE.1.02.006 Unapproved Counter Party	Unapproved counterparties can participate in asset transfers, e.g., high-value asset transactions, that can result in fraud or abuse on the network.
R.GOVERNANCE.1.02.007 Multinode Compromise	Lack of policies to monitor for consensus failure can result in the loss of digital assets, data and/or transaction records. Such failure may result from attacks on the network causing multinode failure, which may prevent or delay consensus being reached.
R-2 Infrastructure 2.01 Software Vulnerabilities 2.02 Protocol Management 2.03 Consensus Mechanism 2.04 Data Management 2.05 Interoperability 2.06 Integration	Any blockchain functionality or capability independent of a data transaction on the blockchain
R-2.01 Software Vulnerabilities	All blockchains use specific algorithms, protocol code and sometimes specific hardware to complete the blockchain life-cycle process. This software can be vulnerable depending on its design and dependencies.
R.INFRASTRUCTURE.2.01.001 Algorithm Vulnerabilities	Poorly designed code may expose vulnerabilities—such as a weakness in a code, cipher, cryptographic protocol or key management scheme—that can be used to circumvent the security of a blockchain cryptographic protocol. Specific vulnerabilities may result in the following: • Risk of a hash collision attack used to search for two input strings of a hash function that produce the same hash result • Unauthorized and/or malicious use of the blockchain network to achieve hostile aggregation of a majority of network processing power, possibly for the goal of illicit monetary gain or to inflict operational or reputational harm to the blockchain and/or participating enterprises • Unintentional errors in data processing • Risk of an attack using cryptoanalysis to determine the wallet address of the sender and receiver in a ring-signature-based blockchain protocol
R.INFRASTRUCTURE.2.01.002 Genesis Block Creation	The formation of a blockchain protocol that uses an inadequately secure ceremony or fails to ensure confidentiality can result in risk to information on the blockchain (e.g., digital assets being subject to misappropriation or misuse by an attacker).

Risk Domain and Subdomain	Risk Description
R.INFRASTRUCTURE.2.01.003 Block Protocols	Protocol violations of block structural constraints may negatively impact the stability or integrity of the blockchain and result in fraud or abuse to the system. These protocol violations include the following: • Block height (number of blocks in a chain from genesis block) exceeds a specified limit. • Subsequent transactions related to previous high-risk transactions can be validated before a certain block depth i.e., number of blocks since the most recently added block, is reached. • Sum of all transactions in a block exceeds the allowable block size, i.e., the allowable amount of data in one block. • Transaction values—both, total value of all transactions, and input or output transaction values—exceed agreed-upon parameters. • Partial or residual transactions are proposed to the blockchain because transaction size in bytes is smaller than the agreed-upon minimum. • Block signer signs multiple blocks at the same block height because there are no limits to signature operations, i.e., signing transactions to validate transactions. • A dependent or referenced input transaction does not have a corresponding output transaction in the current block or in a future block. • Block timestamps are before or after the current system time based on configuration parameters. • Validators are able to anticipate transactions in a block before the block is approved and submitted to the blockchain, which creates a race condition, i.e., accidental collisions due to two validators mining the same block at the same time. • Block signers, i.e., miners, sign multiple blocks at the same height. • The timestamp of a block is manipulated by a block generator, miner or validator. • A dependent transaction, i.e., one that is tied to another transaction, is not completed before it reaches a predefined limit, e.g., 100 blocks, causing a growing transaction depth that may indicate it is an orphan or unauthorized transaction.
R.INFRASTRUCTURE.2.01.004 Software Update (Patching)	Improperly coded updates or patches to the system may result in unintended loss or damage of data, or to unauthorized access to the system.
R.INFRASTRUCTURE.2.01.005 Functions Beyond Permission	A node or a group of nodes in a particular role may gain too much control, power or access due to a lack of system security, i.e., failure to operate as designed, negatively influencing and compromising the integrity, trust and usability of the network. For example, if roles of nodes are improperly defined, creating improper segregation of duties, this may result in nodes acting in a manner that intentionally or unintentionally disrupts or harms the blockchain.
R-2.02 Protocol Management	The blockchain protocol[4] and protocol change management are designed and operated to meet the objectives of the network effectively. The specific risk related to consensus mechanism (a component of protocol) is described in the following subdomain section (see **R-2.03 Consensus Mechanism**).
R.INFRASTRUCTURE.2.02.001 Data Faults	Configuration, network and algorithmic errors may cause data faults, such as blockchain length mismatch, data loss and corruption. These errors can force recalculations for the data that are added to the chain, resulting in slower transaction times, loss of service and chain corruption.
R.INFRASTRUCTURE.2.02.002 System Faults	System faults, such as errors in new node synchronization and node block requests, can lead to system protocol hardware errors that corrupt data, causing loss or latency of service that results in blockchain malfunctions.
R.INFRASTRUCTURE.2.02.003 Asset Issuance Control	Inappropriate approvals of an asset that is added to the blockchain can lead to invalid or fraudulent asset additions.
R.INFRASTRUCTURE.2.02.004 Asset Retirement	Inappropriate approvals of an asset that is disposed or retired from the blockchain can lead to invalid or fraudulent asset deletions.
R.INFRASTRUCTURE.2.02.005 Transaction Sequencing	Failure to follow critical transaction sequencing or timing can result in compromise to the network performance or integrity.
R.INFRASTRUCTURE.2.02.006 Configuration	Configuration changes may adversely impact application programming interfaces (APIs) and other connections, e.g., oracles, that enable improper distribution of information.
R.INFRASTRUCTURE.2.02.007 Protocol Version/Change Management	Lack of an up-to-date release version of the protocol software on a network or a node may cause a business interruption or security compromise of the network, or prevent valid nodes from being able to participate in the network.
R.INFRASTRUCTURE.2.02.008 Error/Activity Logs	A compromise in traceability of procedure or code changes can cause an increase in vulnerabilities to the network protocol.
R.INFRASTRUCTURE.2.02.009 Quorum/Multisig	Circumvented signature requirements or flawed multisignature (multisig) design can result in a compromise of the integrity of the blockchain.

[4] Blockchain protocol is the software that manifests the instructions for nodes on the network and includes instructions for the consensus mechanism.

Risk Domain and Subdomain	Risk Description
R.INFRASTRUCTURE.2.02.010 Time Lock	Errors in the protocol code or smart contracts on the network can cause timed transactions to be executed improperly, which may result in financial loss or liability due to premature or latent transactions.
R.INFRASTRUCTURE.2.02.011 Locking Scripts	Inability to validate unlocking scripts for inputs against the corresponding locking scripts for outputs can adversely affect the integrity of the network and may be an indicator of fraud or abuse.
R.INFRASTRUCTURE.2.02.012 Integer Overflow and Underflow	Network transactions generated by block code or smart contracts may reach integer overflow and underflow limits, which may result in unwanted value resets, fraud or abuse on a blockchain.
R.INFRASTRUCTURE.2.02.013 Run Limits	A network program, e.g., protocol analytics and smart contracts, exceeding its established run limit or "gas" consumption may be indicative of a compromise or fraud against the system.
R.INFRASTRUCTURE.2.02.014 Preventing Infinite Loops	Conditional instructions in protocol or smart contract code, e.g., branches and loops using Jump and Jump if, can allow infinite loops that can put the ongoing operation and integrity of the network at risk.
R-2.03 Consensus Mechanism	The blockchain consensus mechanism should be designed and operated to meet the objectives of the network effectively, and to mitigate fraud or abuse on the network.
R.INFRASTRUCTURE.2.03.001 Multinode Compromise	Multinode compromise can cause a consensus failure that can result in the loss of digital assets, or data and/or transaction records.
R.INFRASTRUCTURE.2.03.002 Fault Tolerance	Insufficient fault tolerance in the consensus mechanism can result in the blockchain not being able to operate if one or more components fail.
R.INFRASTRUCTURE.2.03.003 Transition in Consensus Mechanism	Insufficient support for a change in the consensus mechanism, e.g., a developer community attempts a move from one consensus mechanism to another, can result in a fork, or decrease the overall security of the network by making assets vulnerable or causing transactions to be unreliable.
R.INFRASTRUCTURE.2.03.004 Dominating Nodes	Individual nodes or participants who dominate the network and block production or transactions can compromise a blockchain, causing the blockchain to fail to achieve its mission or objective. For example, an administrative node that has too much control may dominate transactions, processing and verification. In addition, a miner who obtains 51% of the total hashing power of a proof of work (PoW) public blockchain can theoretically initiate a 51% attack.
R.INFRASTRUCTURE.2.03.005 Uptime Risk	A node that is offline for a long period of time may result in the node not matching the network speed, which causes issues with consensus processing. In addition, the risk that the node either transmits incorrect information or is not able to transmit information may increase, which can impair the consensus on the network or cause failure of transactions to process on the blockchain.
R.INFRASTRUCTURE.2.03.006 Node Authorization and Identification	Insufficient identification and authorization procedures may allow unauthorized nodes to access the network. Nodes that are not authorized to verify transactions and communicate verified transactions to other nodes on the network can initiate unauthorized transactions. In addition, authorized nodes can participate in unauthorized transactions and network activity if additional controls are not in place.
R.INFRASTRUCTURE.2.03.007 Node Limits and Transition	Too few nodes on a blockchain may negatively impact the stability or integrity of the blockchain. A network administrator can initially have disproportionate control over the network until additional nodes help the network evolve to an appropriate level of security. An inadequate number of nodes, insufficient roles of nodes and network immaturity can introduce risk that the network lacks security and integrity compared to the roadmap and security claims made by the creators.
R.INFRASTRUCTURE.2.03.008 Multilocation Validator Nodes	Clusters of nodes in one geographical location or in one enterprise can make the network susceptible to a network outage that can decrease network security, transaction throughput and validation.
R.INFRASTRUCTURE.2.03.009 Dynamic Voting	Violation of a voting threshold for a voting consensus mechanism may have a negative impact on block creation or validation.
R.INFRASTRUCTURE.2.03.010 Voting Restrictions	Failure to restrict the number of times a validator can vote in a given time frame can cause biased voting because validator nodes can misuse voting rights or vote twice or more at the same block height. For example, a participant can vote on a block that is higher than the block height. If two blocks are created at the same time, then a participant can vote on both.
R.INFRASTRUCTURE.2.03.011 Inactive Validator Nodes	If validating nodes with no activity for a specified period of time are not removed from the network when they should be, the resulting inefficiencies while the system waits for those nodes to validate transactions can slow down the network.
R-2.04 Data Management	Offchain information that is stored or transmitted in a computer-readable format and used to transact or interact on a blockchain network, or onchain data that are sourced from a blockchain network and treated as a source of truth for a business purpose.
R.INFRASTRUCTURE.2.04.001 Insufficient Storage	Insufficient storage controls for one or more participants, i.e., nodes, may result in security issues in the areas of logical and physical access, and processing integrity.
R.INFRASTRUCTURE.2.04.002 Disclosure of PII	Disclosure of personally identifiable information (PII) or confidential information on a blockchain that is accessed by unauthorized parties can result in inappropriate use of the information.

Risk Domain and Subdomain	Risk Description
R.INFRASTRUCTURE.2.04.003 Disclosure of Blockchain Details	Allowing individuals, i.e., anyone in a public blockchain or participants in a private blockchain, to query the blockchain to obtain details of a transaction can lead to exposure of confidential information or metadata through additional analysis.
R. INFRASTRUCTURE.2.04.004 Masking Identities	A system design that masks participant data that should be available can enable a participant to engage in related party transactions without other participants' knowledge. For example, a participant may use the confidentiality attributes of the blockchain to run two nodes, giving the appearance that the two nodes are run by different individuals. The participant then engages in wash trading or other nefarious actions, to manipulate the market by inflating the trade volume.
R.INFRASTRUCTURE.2.04.005 Capacity/Size of Onchain Transactions	Capacity issues can occur if a blockchain becomes too large, leading to blockchain bloat and network inefficiencies. (See **R-3.03 Blockchain Bloat**.)
R.INFRASTRUCTURE.2.04.006 Incorrect Offchain Data	Incorrect or unreliable offchain data from a blockchain oracle or other external party source can result in incorrect transactions being processed.
R.INFRASTRUCTURE.2.04.007 Right to Be Forgotten	If a participant decides to withdraw from a system, failure to remove all the participant's previously disclosed personal data from a blockchain network, as requested, may violate right to be forgotten regulations.
R-2.05 Interoperability	A computer system can exchange and use data or transfer an asset without any effects on the state or uniqueness of the asset.
R.INFRASTRUCTURE.2.05.001 Accuracy and Completeness	Inaccuracy and incompleteness of transaction data may occur when data are transferred between two systems. Even if blockchain technology enables completeness and accuracy, the endpoint system may have issues that cause risk.
R.INFRASTRUCTURE.2.05.002 Inconsistent Format	Systems may use different formats of data, either preventing the systems from exchanging or using information, or requiring significant resource expenditures to normalize data in the absence of standards or agreed-upon taxonomies.
R.INFRASTRUCTURE.2.05.003 Insufficient Intermediary System Security	Intermediary systems, i.e., systems between the blockchain and other systems, may lack security, or their cybersecurity protocols may be insufficient to prevent hacks and data theft.
R.INFRASTRUCTURE.2.05.004 Technical Trouble in Intermediary Systems	Intermediary systems may experience operational disruptions or other technical failures, which may affect the entire interoperating system processing and efficiency.
R.INFRASTRUCTURE.2.05.005 Offchain Master Data	The offchain master data may not be appropriately managed and secured to ensure validity and integrity.
R-2.06 Integration	Different blockchains, computing systems and software applications are linked physically or functionally, allowing them to act as a coordinated whole.
R.INFRASTRUCTURE.2.06.001 Integration Linkages	Across all domains, risk exists due to inconsistencies in connecting with existing client-server systems (e.g., databases, file servers and message brokers, via existing API, FTP, etc.). The following are possible issues resulting from compromised data inputs in a blockchain platform: • Normalization of data • Missing data • Insufficient block size and throughput capacity • Unauthorized entry of data • Data inputs and reference data definitions that conflict across multiple systems • Loss of anonymity or compromised/stolen data that are ported across multiple linkages • Integration with identity management systems
R.INFRASTRUCTURE.2.06.002 Data Integrity	The sharing of data and normalization of data between blockchains and legacy systems of insufficient integrity may cause integration difficulties or issues with data format and alignment. For example, if a data transfer between a blockchain and a legacy system results in data being unmatched or missing, it may be challenging to make corrections after transactions are recorded, due to the immutability of blockchains.
R.INFRASTRUCTURE.2.06.003 Integration Points	The nature of a blockchain and the inflexibility of the architecture of legacy systems may limit potential solutions to integration challenges, such as unknown or undocumented integration points. This may result in the inability of a blockchain system to connect, send or receive relevant information for processing.
R.INFRASTRUCTURE.2.06.004 Infrastructure	An inadequate integration infrastructure may cause system failure, e.g., inadequate quantity or insufficient processing power of physical systems, such as hardware, storage, routers and switches, or software inherent in the blockchain implementation.
R.INFRASTRUCTURE.2.06.005 Change Management	Inadequate or unaligned change management procedures can make it difficult or impossible to determine if legacy or blockchain infrastructure changes will adversely affect the systems integration and platform.
R.INFRASTRUCTURE.2.06.006 Integration Testing	Inadequate integration testing plans may prevent proper functioning of the systems or platforms.
R.INFRASTRUCTURE.2.06.007 Integration Planning	Insufficient knowledge of blockchain technology within an enterprise can negatively impact integration planning and implementation. For example, it may cause the loss of master or transactional data, or prevent the capture of relevant data or the protection of PII and confidential data.

Risk Domain and Subdomain	Risk Description
R.INFRASTRUCTURE.2.06.008 Integration Schedules	Failure of a blockchain platform process to align with existing integration system schedules, e.g., reset or downtime, and system upgrades, can impact all data types that are not aligned to those schedules.
R.INFRASTRUCTURE.2.06.009 Integration Architecture	The network integration architecture of the blockchain and legacy systems may be incomplete, obsolete or inflexible, and, thus, unable to facilitate changes or upgrades.
R.INFRASTRUCTURE.2.06.010 Quality and Normalization of Data	The quality and normalization of data to be shared between blockchains and legacy systems may be inadequate to allow blockchain tech stacks to reach the same data points and conclusions. The resulting unmatched or missing data can cause integration difficulties, input validity issues or intentional/unintentional inclusion of unauthorized PII and confidential information.
R.INFRASTRUCTURE.2.06.011 Cross Network Interactions	Conducting cross-network interactions, e.g., those with side or child chains, outside approved networks or beyond approved limits may compromise the parent network data, integrity or security.
R-3 Data 3.01 Data Integrity 3.02 Access Rights 3.03 Blockchain Bloat 3.04 Nonstandard Transactions 3.05 Data Output 3.06 Out of Range Data 3.07 Orphan Address	Offchain information that is stored or transmitted in a computer-legible format and used to transact or interact on a blockchain network, or onchain data that are sourced from a blockchain network and treated as a source of truth for a business purpose
R-3.01 Data Integrity	Incomplete, inaccurate or unauthorized data transmitted or compiled to create a blockchain transaction and sourced by an entity from a node can result in fraudulent data, data input or processing errors, missing data, duplicate data or unauthorized entries, e.g., the input and output values of the data in the block and the sums of the data in the block are outside allowable ranges.
R-3.02 Access Rights	Unauthorized or improperly permissioned client access to database, server or parser application resources that transmit, compile or translate data to create a blockchain transaction or record can result in fraudulent data, data input or processing errors, missing data, duplicate data or unauthorized entries.
R-3.03 Blockchain Bloat	As a blockchain grows over time, data storage requirements may not be met, resulting in disruptions to the network. (See **R.INFRASTRUCTURE.2.04.005 Capacity/Size of Onchain Transactions**.)
R-3.04 Nonstandard Transactions	Approval of nonstandard transactions, e.g., transactions that are not aligned with the blockchain design or use case, may compromise the data available on the network and potentially facilitate fraud.
R-3.05 Data Output	Data output, e.g., metadata such as purchase order numbers, that is missing or misplaced, i.e., existing in another transaction where it does not belong, can have an adverse effect on the integrity of the data or network, resulting in fraud or abuse.
R-3.06 Out-of-Range Data	Allowing input and output values of block data or block data sums that are outside allowable ranges can adversely affect the availability and integrity of the data and may be an indicator of fraud or abuse.
R-3.07 Orphan Address	Lack of processes to check the validity of a recipient's blockchain address when sending transactional information or tokens can result in the information or tokens being sent to an address that does not exist or is inaccessible, i.e., orphan address.
R-4 Key Management 4.01 Insufficient Entropy 4.02 Key Creation Methodology Validation 4.03 Key Ceremony 4.04 Third-party Created Keys 4.05 In-use Key Security 4.06 Key Encryption When Not In Use 4.07 Key Backup Existence 4.08 Geographic Key Backups 4.09 Key Backup Access Controls 4.10 Key Backup Environmental Protection 4.11 Key Compromise Protocol 4.12 Keyholder Grant/Revoke Policies 4.13 Usage of Known Identifiers 4.14 SMS Used as 2FA 4.15 Multisig Implementation 4.16 Strong Encryption 4.17 HSM Settings 4.18 Recovery Process 4.19 Hardware Wallet Used for Cold Storage	Management of public and private keys

Risk Domain and Subdomain	Risk Description
R-4.01 Insufficient Entropy[5]	Creating a key/seed with insufficient entropy can place all future use of the keys for storing and transacting in crypto assets at risk. The keys can be brute forced or guessed, resulting in a loss of assets.
R-4.02 Key Creation Methodology Validation	If key/seed creation methodology is not validated prior to creation, keys can be generated without enough entropy, resulting in a loss of crypto assets.
R-4.03 Key Ceremony	The formation of a blockchain protocol using an inadequately secure key ceremony can subject the blockchain to access risk, e.g., digital assets being misappropriated or misused by an attacker.
R-4.04 Third-party Created Keys	If the key/seed is not created by the operator or owner, the key may be compromised by weaknesses in the third-party key management controls, increasing the risk of third-party fraud.
R-4.05 In-use Key Security	Insufficient protection of in-use keys, e.g., for initiating a transaction, can result in unauthorized transactions, loss of assets, or funds being frozen if assets are sent to an invalid address.
R-4.06 Key Encryption When Not In Use	If protection, e.g., encryption and security, is inadequate when keys are not in use, keys can be lost. The results can include funds being accessed or frozen, and transactional information or digital assets being compromised or stolen.
R-4.07 Key Backup Existence	If a key is lost and there is no key/seed backup, i.e., primary key is the only key in existence, the result can be a complete loss of the ability to engage in transactions, loss of digital assets or frozen funds.
R-4.08 Geographic Key Backups	If the primary key and the backup are stored in the same geographic location, an act of God or other incident may cause both sets of keys to be lost at the same time, resulting in the loss of the ability to engage in transactions, the loss of digital assets or frozen funds.
R-4.09 Key Backup Access Controls	The lack of proper physical and logical access controls for primary and backup keys can result in compromise to the keys and unauthorized access.
R-4.10 Key Backup Environmental Protection	If the primary key is lost or compromised and protection of the backup key/seed from environmental risk, such as fire, flood, theft or other acts of God, is inadequate, the result can be loss of assets or funds being frozen. For example, if the backup is stored on paper, rather than on stainless steel or titanium, then the key can be lost due to water damage, degradation of the paper or fire.
R-4.11 Key Compromise Protocol[6]	Lack of key compromise protocols (KCP) for unauthorized modifications can result in an entity not being able to respond to a compromise or the creation of vulnerabilities, leading to potential fraud or abuse on the network or to loss of digital assets.
R-4.12 Keyholder Grant/Revoke Policies	Improper keyholder grant and revoke policies and procedures can lead to someone gaining improper access to keys, resulting in unauthorized movement of assets. This can occur during onboarding and especially during offboarding of staff.
R-4.13 Usage of Known Identifiers	Use of an easily known identifier, e.g., a commonly used email address or phone number, as a user account name reduces the effectiveness of user authentication and thereby increases the risk of user account compromise.
R-4.14 SMS Used as 2FA	A phone number that is used for short message service (SMS) two-factor authentication may be subject to a subscriber identity module (SIM) swapping attack, which can result in transactional information or digital assets being compromised.
R-4.15 Multisig Implementation	If a multisignature (multisig) scheme is not appropriately designed or implemented, or not deployed when appropriate, then custody and authorization can reside with one party or the multisig scheme may be bypassed, allowing a party to create an inappropriate transaction, including misappropriation of digital assets.
R-4.16 Strong Encryption	Use of encryption algorithms that are not widely recognized as providing strong encryption to store or transmit keys may allow exploitation of unknown vulnerabilities, resulting in a hostile actor obtaining plain text keys and creating inappropriate transactions, including misappropriation of digital assets.
R-4.17 HSM Settings	Use of hardware security module (HSM) configurations that do not comply with industry-standard security settings may result in vulnerabilities that can be exploited to obtain plain text keys and create inappropriate transactions, including misappropriation of digital assets.
R-4.18 Recovery Process	Insufficient testing to identify and correct flaws in a key recovery process can result in failure to recover keys in the event of an incident.
R-4.19 Hardware Wallet Used for Cold Storage	Failure to use hardware wallets appropriately for cold storage may allow the creation of inappropriate transactions, including misappropriation of assets.
R-5 Smart Contracts 5.01 Governance Risk 5.02 Design Risk 5.03 External Interaction Risk 5.04 Manipulation/Denial of Service Risk	Blockchain networks and other distributed-ledger technology that run virtual machines and decentralized code, and allow for programmatic value transfer and recording of state and other transaction data

[5] The concept of entropy signifies a lack of order or predictability.
[6] Key compromise protocols may include an inventory of keys, processes and procedures, knowledgeable personnel and authenticated communication channels to be executed for the mitigation of damages when an encryption key has or may have been compromised.

Risk Domain and Subdomain	Risk Description
R-5.01 Governance Risk	Smart contract (SC) governance risk is regulatory or legal risk inherent in the design and operation of any SC with the potential to trigger compliance or legal actions against the network designers/participants.
R.SMARTCONTRACT.5.01.001 Violations of Contract Law/Regulation	Contractual obligations hard coded in the SC code and approved by the consensus mechanism of the network may violate contract law/regulation, creating conflicts with contract law in multiple jurisdictions and resulting in the contract becoming unenforceable in any of the jurisdictions in which the SC operates or may operate.
R.SMARTCONTRACT.5.01.002 Digital Assets Risk	Digital assets transacted by the SC may not be permissible in one or more of the jurisdictions in which the SC operates, resulting in violations of regulations.
R.SMARTCONTRACT.5.01.003 Regulatory and Legal Jurisdiction	The borderless nature of the SC/network may create ambiguity about the regulatory and legal jurisdiction of the SC/network, resulting in reporting, i.e., tax and financial, issues and regulatory compliance risk in multiple jurisdictions.
R.SMARTCONTRACT.5.01.004 Decentralization Reporting/Regulatory Risk	The decentralized nature of a blockchain network on which SCs operate may result in a lack of clarity about which entity or individual is responsible for reporting or ensuring regulatory compliance.
R.SMARTCONTRACT.5.01.005 Privacy Risk	SC transactions or outputs to the network may not appropriately protect and secure personally identifiable information (PII) that is regulated under privacy laws around the world, e.g., General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), resulting in privacy liability for the blockchain and participants.
R-5.02 Design Risk	Smart contract (SC) design risk is ubiquitous risk inherent in the design of any SC with the potential to compromise the intended SC function, including risk applicable to any software code.
R.SMARTCONTRACT.5.02.001 Circuit Breaker/Self-Destruct Protection	The lack of adequate circuit breaker/self-destruct detection and mitigation protections during processing that are consistent with the design of the SC can result in large or undetected losses/liability.
R.SMARTCONTRACT.5.02.002 Transaction Limits	Inadequate SC transaction limits, i.e., high or low, can result in large or undetected losses/liability.
R.SMARTCONTRACT.5.02.003 Change Management	The consensus approved change management process for adding or upgrading SCs may introduce wrong or malicious code or sequencing in an SC, resulting in contract performance or network liability damage to the nodes or network participants.
R.SMARTCONTACT.5.02.004 Time Lock/Lock Time SC Transactions	Design errors in Time Lock/Lock Time coding, i.e., parameters for execution, may cause premature or latent transactions, resulting in financial losses/liability.
R.SMARTCONTACT.5.02.005 Source of Randomness	Failure to use a strong source of randomness, which is difficult to achieve in Ethereum, can make a SC vulnerable to hacker attacks and manipulation, especially when using onchain data.
R.SMARTCONTACT.5.02.006 Timestamp Dependence	Functions of a SC that are triggered by time variables from the blockchain, such as block.timestamp and block.number, can be manipulated by a miner.
R.SMARTCONTACT.5.02.007 Hash Collisions	The use of a soft or inadequate encryption tool or methodology, e.g., MD5 and SHA vs. SHA-256, can cause hash collisions that can result in large or undetected losses/liability.
R.SMARTCONTACT.5.02.008 Deprecated Functions and Outdated Compiler Versions	The use of deprecated functions or outdated compiler versions can make the SC logic vulnerable to attacks.
R-5.03 External Interaction Risk	The SC's interactions with other SCs (including itself if run before the first version finishes), data, oracles, or other processes or network features can create unforeseen vulnerabilities, resulting in a compromise of the SC and the network.
R.SMARTCONTRACT.5.03.001 Reentrancy[7]	Reentrancy risk can result from many types of SC program calls. A key vulnerability involves functions that can be called repeatedly, before the first invocation of the function is finished, which may cause different invocations of the function to interact in destructive ways.
R.SMARTCONTRACT.5.03.002 Race Conditions[8]	Race conditions describe a form of reentrancy that creates risk when independent SC codes, which may be secure running alone, are run simultaneously or out of order, creating unforeseen anomalies.
R.SMARTCONTRACT.5.03.003 Delegate Call Injection	A malicious callee contract, i.e., the invoking contract, can directly modify or manipulate the state variables of the caller contract by updating the bytecode of a callee contract, which may result in fraud or abuse.
R.SMARTCONTRACT.5.03.004 Denial of Service with Unexpected Revert	A callee contract can revert a transaction, resulting in value loss or nonperformance of a contract, e.g., when a caller contract encounters a failure in an external call, or the callee contract deliberately performs the revert operation to disrupt the execution of the caller contract.
R.SMARTCONTRACT.5.03.005 Call Exception Management	Unintentional or malicious mishandling of SC call exceptions can result in erroneous or unintended transactions, causing failure of the contract or financial loss to the network.
R.SMARTCONTRACT.5.03.006 Smart Contract Owner Compromise	A nefarious actor can call a vulnerable SC function to take over ownership, compromising the SC author/owner's address and resulting in a loss of ownership.

[7] Call reentrancy refers to all functions that can be repeated, prior to the first call function finishing.
[8] Race conditions are created when a software program that relies on the timing of one or more processes to function correctly is able to run out of sequence.

Risk Domain and Subdomain	Risk Description
R.SMARTCONTRACT.5.03.007 Third-Party External Inputs	SCs may rely on insecure, inaccurate or inappropriately accredited oracles to provide critical third-party external inputs, e.g., via a System and Organization Controls (SOC) review, resulting in contract violations/failure.
R-5.04 Manipulation/Denial of Service Risk	Manipulation/Denial of Service Risk is any potential SC vulnerability, originating from within or outside the network, that might allow manipulation of data on the network or restriction of a node or user access to the network.
R.SMARTCONTRACT.5.04.001 Frozen Funds	Failure to provide contracts with a function for spending funds and instead relying on the fund-spending function of another contract can result in users being unable to spend funds deposited into their contract accounts, effectively freezing their funds and preventing them—either accidentally or deliberately—from performing on a contract or obligation.
R.SMARTCONTRACT.5.04.002 Manipulated Balance	Manipulation of fee balances to or away from contracts can result in a denial of access or denial of services attack, e.g., when a contract control-flow decision relies on the value of a particular balance or address that an attacker can leverage, potentially resulting in fraud or abuse.
R.SMARTCONTRACT.5.04.003 Erroneous Function Labeling	An incorrectly specified function, e.g., a function that is not labeled private or internal with appropriate encryption, may permit unauthorized access, resulting in fraud or abuse to the system.
R.SMARTCONTRACT.5.04.004 Caller Identity Validation	Failure to check and validate a caller's identity when the caller invokes a function to send fees to an arbitrary address can result in contract funds being withdrawn by a caller who is neither the owner of the contract nor an investor who deposited funds in the contract.
R.SMARTCONTRACT.5.04.005 Suppression/Stuffing Attacks	Sending multiple transactions with high fee prices and limits to SCs that assert (or use other means) to consume all the fees and fill up the block fee limits can stop or delay others from running transactions, resulting in the potential for loss or abuse on the network.
R.SMARTCONTRACT.5.04.006 Unexpected Throws	In any type of bidding or group payment transaction, a malicious bidder may throw or take over the transaction, which can result in an incomplete transaction with no one getting paid, refunded, or winning a bid.
R.SMARTCONTRACT.5.04.007 Fee Limits	Manipulating fees to exceed system limits, i.e., the ceiling for the amount of fees that can be spent, may cause a transaction to fail, leading to possible denial of service. Excessive use of fees by a single node or user to execute SCs may be an indication of fraud or abuse on the network.
R.SMARTCONTRACT.5.04.008 Conflicting Transactions	Competing transactions/contacts, e.g., one is canceling an order while another is trying to fulfill the same order, or one transaction/contact is running a large bulk transaction while another is trying to procure a small part of that bulk processing, may result in delayed, canceled or incomplete contracts.
R.SMARTCONTRACT.5.04.009 Poisoning	Placing nefarious information, e.g., fraudulent data, computer viruses and malware, PII or other private information on a blockchain via transaction combinations or SCs may result in violations of compliance standards, e.g., General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).
R.SMARTCONTRACT.5.04.010 Transaction Order/Front Running	Miners or administrators with insider knowledge of block or mempool transactions can engage in front running on blockchains/smart contracts before they are submitted to the ledger, resulting in financial losses. For example, a transaction to buy tokens is seen, and a market order is implemented before the transaction is included, due to insider trading activities.
R.SMARTCONTRACT.5.04.011 Signature Verifications	Signatures created offchain and validated using SC code may be intercepted and parameters modified to match other valid signatures, resulting in undetected losses/liabilities.
R.SMARTCONTRACT.5.04.012 Malicious Transaction Relayer	In a smart contract that has provisions for transaction relaying,[9] the relayer can censor transactions by allocating a sufficient amount of gas for the relay function to execute successfully but not enough for the final transaction to succeed.

[9] Transaction relaying is used when an entity wants to make a transaction but cannot execute it directly because of some limitations, e.g., the transaction sender wants to transfer some ERC20 tokens but does not have Ether to pay for gas costs. The third-party relayer submits the sender's presigned transaction to the network.

What's Next?

Since the inception of the first blockchain in 2009, there has been a Cambrian explosion of innovation—in new business models built around new blockchain protocols and in applications of blockchain to longstanding operational, trust and transparency issues across traditional industries. The trend is clear: More and more enterprises will experiment—and eventually transform—significant portions of their business, revenue model or operations using blockchain.

Decisions to implement blockchain technology should be made only after carefully assessing the risk. If blockchain has already been implemented, enterprises should perform retrospective reviews to identify risk related to governance, infrastructure, data, key management and smart contracts, as applicable, and surface any control gaps that may jeopardize enterprise objectives.

Appendix A: ISACA and AICPA & CIMA Blockchain Resources

ISACA and AICPA & CIMA offer the following resources to help practitioners increase their blockchain knowledge.

White papers	• Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession • CPAs Leveraging Blockchain Technology • Blockchain and Internal Control: The COSO Perspective • Implications of the Use of Blockchain in SOC for Service Organization Examinations • Blockchain—An Executive View
Continuing professional education (CPE)	• Blockchain for Digital Assets: Accounting for Digital Assets Under U.S. GAAP • Digital Mindset Pack (2019-20)
Certificate programs	• Blockchain and Beyond: Blockchain for Accounting and Finance Professionals Learning Programs • Certified in Emerging Technology: Blockchain Fundamentals
Other resources	• Blockchain Universal Glossary • Blockchain Preparation Audit Program • Blockchain Fundamentals • Blockchain Legislation Emerging in State Legislatures • Emerging Technology Report: Blockchain • ISACA Blockchain Framework and Guidance • How will blockchain change accounting? • Blog posts • 2020 Blockchain Symposium: The Emerging Technology is Maturing as Real-World Applications Expand

Acknowledgments

ISACA and AICPA & CIMA wish to acknowledge:

ISACA-AICPA & CIMA Joint Blockchain Working Group

Rory Alsop
HSBC Holdings plc

Ami Beers
The Association of International Certified Professional Accountants, representing AICPA & CIMA

Gerard (Rod) Brennan
Lukka

Dustin Brewer
ISACA

Noah Buxton
Armanino

Andres Castaneda
GT

Ray Cheung
Crowe

Tim Davis
Deloitte

Shannon Donahue
ISACA

Wesley Freeman
BDO

Yasmine Hakimpour
CPA Canada

Chris Halterman
EY

Mike Krajecki
KPMG

Diana Krupica
The Association of International Certified Professional Accountants, representing AICPA & CIMA

Erin Mackler
The Association of International Certified Professional Accountants, representing AICPA & CIMA

Kirk Phillips
Global Crypto Advisors

Ron Quaranta
Wall Street Blockchain Alliance

Rolf Von Roessing
Forfa Consulting

Jeannette Russell-Shepherd
Friedman

Amy Vetter
The B3 Method Institute

Tim Virtue
Independent Contractor

Bernie Wieger
KPMG

ISACA Board of Directors

Tracey Dedrick, Chair
Former Chief Risk Officer, Hudson City Bancorp, USA

Rolf von Roessing, Vice-Chair
CISA, CISM, CGEIT, CDPSE, CISSP, FBCI
Partner, FORFA Consulting AG, Switzerland

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Pam Nigro
CISA, CRISC, CGEIT, CRMA
Vice President–Information Technology, Security Officer, Home Access Health, USA

Maureen O'Connell
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

David Samuelson
Chief Executive Officer, ISACA, USA

Gerrard Schmid
President and Chief Executive Officer, Diebold Nixdorf, USA

Gregory Touhill
CISM, CISSP
President, AppGate Federal Group, USA

Asaf Weisberg
CISA, CRISC, CISM, CGEIT
Chief Executive Officer, introSight Ltd., Israel

Anna Yip
Chief Executive Officer, SmarTone Telecommunications Limited, Hong Kong

Brennan P. Baybeck
CISA, CRISC, CISM, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM
ISACA Board Chair, 2018-2019
Independent Director, Titus, and Executive Chair, White Cloud Security, USA

Chris K. Dimitriadis, Ph.D.
CISA, CRISC, CISM
ISACA Board Chair, 2015-2017
Group Chief Executive Officer, INTRALOT, Greece

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams that effectively drive IT audit, risk management and security priorities forward. ISACA is a global professional association and learning organization that leverages the expertise of more than 150,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide. In 2020, ISACA launched One In Tech, a philanthropic foundation that supports IT education and career pathways for under-resourced, under-represented populations.

About the Association of International Certified Professional Accountants and AICPA & CIMA

The Association of International Certified Professional Accountants® (the Association) is the most influential body of professional accountants, combining the strengths of the American Institute of CPAs® (AICPA®) and The Chartered Institute of Management Accountants® (CIMA®) to power trust, opportunity and prosperity for people, businesses and economies worldwide. It represents 650,000 members and students across 179 countries and territories in public and management accounting, and advocates for the public interest and business sustainability on current and emerging issues. With broad reach, rigor and resources, AIPCA & CIMA advances the reputation, employability and quality of CPAs, CGMAs and accounting and finance professionals globally.

DISCLAIMER

ISACA and AICPA & CIMA have designed and created *Blockchain Risk: Considerations for Professionals* (the "Work") primarily as an educational resource for professionals. ISACA and AICPA & CIMA make no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Phone: +1.847.660.5505
Fax: +1.847.253.1755
Support: support.isaca.org
Website: www.isaca.org

AICPA & CIMA
Worldwide leaders in public and management accounting
220 Leigh Farm Road
Durham, NC 27707, USA
Phone: 1.888.777.7077
Fax: 1.888.233.7618
Support: www.aicpa.org/help.html
Website: www.aicpa.org

Provide Feedback:
www.isaca.org/blockchain-risk

Participate in the ISACA and AICPA & CIMA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews
www.twitter.com/AICPA

LinkedIn:
www.linkedin.com/company/isaca
www.linkedin.com/company/aicpa/

Facebook:
www.facebook.com/ISACAGlobal
https://www.facebook.com/AICPA

Instagram:
www.instagram.com/isacanews/
www.instagram.com/theaicpa