



Committee of Sponsoring Organizations of the Treadway Commission

Governance and Internal Control



# BLOCKCHAIN AND INTERNAL CONTROL

THE COSO PERSPECTIVE

Sponsored By

**Deloitte.**

**Jennifer Burns | Amy Steele | Eric E. Cohen | Dr. Sri Ramamoorti**

The information contained herein is of a general nature and based on authorities that are subject to change. Applicability of the information to specific situations should be determined through consultation with your professional adviser, and this paper should not be considered substitute for the services of such advisors, nor should it be used as a basis for any decision or action that may affect your organization.

## Authors



**Jennifer Burns**  
Partner  
Deloitte & Touche LLP



**Amy Steele**  
Partner  
Deloitte & Touche LLP

## Contributing Authors



**Eric E. Cohen**  
Cohen Computer  
Consulting



**Dr. Sri Ramamoorti**  
Associate Professor  
University of Dayton

## Acknowledgements

We would like to recognize and thank Yoland Sinclair, Manager, Deloitte & Touche LLP, the COSO Board, and COSO Chairman Paul Sobel for providing input, assistance, and valuable feedback in developing this paper. We also thank Tim Davis, Principal, Shelby Murphy, Managing Director, and Gireesh Sivakumar, Senior Manager, Deloitte & Touche LLP for their technical input and advice.

The COSO Board would like to thank Dr. Sri Ramamoorti for originating the idea for this paper and Deloitte & Touche LLP for its support.

## COSO Board Members

**Paul J. Sobel**  
COSO Chair

**Daniel C. Murdock**  
Financial Executives International

**Douglas F. Prawitt**  
American Accounting Association

**Jeffrey C. Thomson**  
Institute of Management Accountants

**Robert D. Dohrer**  
American Institute of CPAs (AICPA)

**Richard F. Chambers**  
The Institute of Internal Auditors

## Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by the following organizations:



**American Accounting Association (AAA)**



**American Institute of CPAs (AICPA)**



**Financial Executives International (FEI)**



**The Institute of Management Accountants (IMA)**



**The Institute of Internal Auditors (IIA)**

**COSO**

Committee of Sponsoring Organizations  
of the Treadway Commission

[coso.org](http://coso.org)

Governance and Internal Control



# BLOCKCHAIN AND INTERNAL CONTROL

THE COSO PERSPECTIVE

Research Commissioned by



Committee of Sponsoring Organizations of the Treadway Commission

July 2020

Copyright © 2020, Committee of Sponsoring Organizations of the Treadway Commission (COSO).  
1234567890 PIP 198765432

COSO images are from the COSO Internal Control - Integrated Framework ©2013, The American Institute of Certified Public Accountants on behalf of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is a trademark of the Committee of Sponsoring Organizations of the Treadway Commission.

All Rights Reserved. No part of this publication may be reproduced, redistributed, transmitted, or displayed in any form or by any means without written permission. For information regarding licensing and reprint permissions, please contact the American Institute of Certified Public Accountants, which handles licensing and permissions for COSO copyrighted materials. Direct all inquiries to [copyright-permissions@aicpa-cima.com](mailto:copyright-permissions@aicpa-cima.com) or AICPA, Attn: Manager, Licensing & Rights, 220 Leigh Farm Road, Durham, NC 27707 USA. Telephone inquiries may be directed to 888-777-7077.

Design and production: Sergio Analco.

<b>Contents</b>	<b>Page</b>
<b>Executive Summary</b>	1
<b>I. Introduction</b>	3
<b>II. The Wave of Change Known as Blockchain</b>	4
<b>III. Components and Principles Overview</b>	7
<b>Conclusion and Next Steps</b>	20
<b>Appendix 1. Technical Appendix</b>	22
<b>Appendix 2. Key Insights: 10 Things to Know About Blockchain</b>	25
<b>Appendix 3. Blockchain, Financial Reporting Assertions, and Audit Evidence</b>	27
<b>Supplementary Resources and References, including those provided by COSO Bodies</b>	29
<b>About the Authors</b>	30
<b>About COSO</b>	32
<b>About Deloitte</b>	32

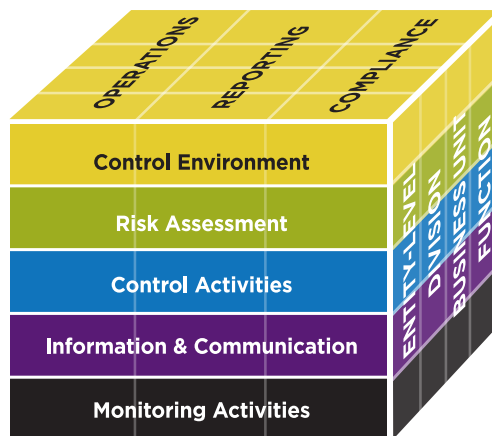




## EXECUTIVE SUMMARY

As blockchain becomes more mainstream, it is appropriate to focus on how this technology intersects with an entity's internal control. With careful implementation and integration of blockchain, the distinctive capabilities of blockchain can be leveraged to create more robust controls for organizations. Further, blockchain-enhanced tools have the potential to promote operational efficiency and effectiveness, improve reliability and responsiveness of financial and other reporting, and improve compliance with laws and regulations. At the same time, blockchain creates new risks and the need for new controls. The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Internal Control — Integrated Framework (2013 Framework)*, see Figure 1) provides an effective and efficient approach that can be leveraged to design and implement controls to address the unique risks associated with blockchain.

Figure 1. The COSO 2013 Framework



When an organization evaluates the use of blockchain through a COSO lens, it enables the board of directors and senior executives to better understand the context and make more informed assessments of the technology's potential and applicability with respect to internal control. This enables the organization to perform a detailed risk analysis and, in turn, develop appropriate control activities to address such risks, facilitating the effective adoption and use of blockchain.

This paper provides perspectives for using the *2013 Framework* to evaluate risks related to the use of blockchain in the context of financial reporting and to design and implement controls to address such risks. It is intended to help inform decisions regarding oversight, risks, and internal control over financial reporting (ICFR). As such, this paper is expected to be of value to the various stakeholders involved in financial reporting, within the context of their own environments (see Table 2). It is not the aim of this paper to explain the intricacies of blockchain nor detail technical differences between the major platforms. Appendix 1, however, includes a discussion of some of the key concepts as used in this paper (concepts in Appendix 1 are in bold the first time they appear in the Executive Summary and in the body of the paper) and the Supplementary Resources and References includes additional resources.

### Observations and Implications

One of the more significant changes resulting from the use of blockchain relates to the hierarchy of the entity. Although the highest level of the hierarchy expressed in the *2013 Framework* as shown in Figure 1 is the Entity Level, drilling down to Division, Operating Unit, and Function, blockchain has the ability to create new collaborative units, spanning different entities, operating on a decentralized basis but bound together with shared data (i.e., a **decentralized database**). From shared ledgers and record-keeping to overarching governance (perhaps leveraging **smart contracts** for oversight and cross-organization internal controls), blockchain can change the concept of an "entity" in an internal control environment as well as the related responsibilities and requirements.

The three objectives of the *2013 Framework*, Operations, Reporting, and Compliance, may be heavily impacted by blockchain in terms of how the objectives are achieved. In particular, many advocates believe that record-keeping will be entirely transformed, leading to completely *ad hoc*, automated, and on-demand reporting and compliance activities. With those transformations, the role and skillsets of management, management accountants, financial executives, and internal and external auditors may be subject to change.

Further, the introduction of blockchain into the business environment will have implications for the five components of the 2013 Framework as follows:

Table 1. Implications of Blockchain on Five Components

Component	Implications of Blockchain
<b>Control Environment</b>	Blockchain may be a tool to help facilitate an effective control environment (e.g., by recording transactions with minimal human intervention). However, many of the principles within this component deal primarily with human behavior, such as management promoting integrity and ethics, which, even with other technologies, blockchain is not able to assess. The greater challenge relates to the intertwining of an entity with other entities or persons participating in a blockchain and how to manage the control environment as a result.
<b>Risk Assessment</b>	Blockchain creates new risks and simultaneously helps to mitigate extant risks, by promoting accountability, maintaining record integrity, and providing an irrefutable record (i.e., a person or organization cannot deny or contest their role in authorizing/sending a message or record).
<b>Control Activities</b>	Blockchain can act as a tool to help facilitate control activities. Blockchain and smart contracts can be a powerful means of effectively and efficiently conducting global business (e.g., by minimizing human error and opportunities for fraud). The collaborative aspects of blockchain, however, can introduce additional complexity, particularly when the technology is decentralized and there is no single party accountable for the systems that fall under ICFR.
<b>Information &amp; Communication</b>	The inherent attributes of blockchain promote enhanced visibility of transactions and availability of data, and can create new avenues for management to communicate financial information to key stakeholders faster and more effectively. One aspect, in particular, for management to consider in applying blockchain is the availability of information to support the financial books and records, and related auditability of information transacted on a blockchain.
<b>Monitoring Activities</b>	The promise of blockchain to facilitate monitoring more often, on more topics, in more detail, may change practice considerably. The use of smart contracts and standardized business rules, in conjunction with Internet of Things (IoT) devices, may alter how monitoring is performed.

### The Future of Blockchain and Its Impacts on Financial Reporting and ICFR

The uses of blockchain will continue to develop and evolve and expanded adoption will likely transform how businesses operate. Many have expressed guarded optimism about the potential effect of blockchain on financial reporting and internal control. As with any disruptive technology, there is a need for each organization, in its own specific context, to evaluate the challenges, better understand the related risks, and work together to determine the best course of action and remediate those risks.

Many of the changes that proponents attribute to the adoption of blockchain are not found in isolation; it is blockchain plus something that is most successful. As a foundational technology, blockchain has the potential to radically change the global digital business landscape that would, in turn, have significant impact on almost everything else.

As organizations are contemplating the use of blockchain, they should know the following 10 things (See Appendix 2 for additional discussion):

- 1 Information about blockchain in the news and on the Internet is often misleading or incorrect.
- 2 Blockchain encompasses far more than **digital assets**; the benefits it can bring to an organization can be substantial.

- 3 Blockchain is not magic; it comes at a cost and doesn't eliminate all risks. In fact, it introduces new risks.
- 4 Knowing how blockchain works is crucial for evaluating, preparing for, and managing blockchain's impact on internal control and the organization as a whole.
- 5 Blockchain has both technology and governance implications.
- 6 Blockchain will not make management, accountants, or auditors less relevant, although it will impact what they do and how they do it.
- 7 Blockchain requires new skill sets (e.g., data science for greater hindsight, insight, and foresight) and new collaboration within and across organizations.
- 8 Now is the time to educate and engage stakeholders throughout the organization.
- 9 Blockchain is still in flux and continues to evolve.
- 10 Adoption of blockchain may not be a choice.

The potential benefits of blockchain to financial reporting will be maximized only if those who understand and are responsible for financial reporting, internal controls, and auditing are actively involved in the discourse about blockchain and collaborate to advance the collective agenda.



## I. INTRODUCTION

This paper describes the use of the COSO Internal Control – Integrated Framework (*2013 Framework*) to evaluate risks related to blockchain<sup>1</sup> in the context of financial reporting and to design controls to address such risks. Although this paper provides a discussion of high-level concepts related to blockchain (some of which are explained in Appendix 1),

this paper is not intended to be a comprehensive guide about blockchain or about all issues, risks, and internal controls associated with the use of blockchain. The following table provides additional context on the audience and intended use of this paper.

Table 2. Audience and Intended Use	
Audience	Intended Use
Board of directors	Understanding the following (governance level): <ul style="list-style-type: none"> <li>• Key concepts related to blockchain</li> </ul>
Audit committee members	<ul style="list-style-type: none"> <li>• How blockchain may impact internal control at a sufficient level to enhance oversight responsibilities</li> </ul>
Executives (CEO, CFO, Controllers)	Understanding of the following (operational and/or technical level): <ul style="list-style-type: none"> <li>• Key concepts related to blockchain</li> </ul>
Internal auditors, management accountants, and others concerned with internal control matters	<ul style="list-style-type: none"> <li>• How to leverage the <i>2013 Framework</i> to evaluate considerations related to the use of blockchain and make more informed decisions about using blockchain</li> <li>• Examples of how each component of the <i>2013 Framework</i> may be impacted when blockchain is implemented</li> </ul>
External auditors	Understanding of the following: (operational and/or technical level) <ul style="list-style-type: none"> <li>• Key concepts related to blockchain</li> <li>• How to evaluate management's controls with respect to blockchain</li> </ul>
Academics	Understanding the following (depending on basic or applied research interest): <ul style="list-style-type: none"> <li>• Key concepts related to blockchain</li> <li>• How blockchain may impact internal controls</li> <li>• How to share the concepts as well as practical applications with students</li> </ul>

This paper discusses each of the COSO components, describing:

- how to use blockchain to enhance that component,
- new threats or risks that arise from using blockchain, and
- examples of how to mitigate such threats or risks.

Finally, with a view to enhancing collaboration, the paper concludes with next steps that can be taken as blockchain becomes more widely adopted.

<sup>1</sup> The term "blockchain" is used throughout this paper to reference blockchain and distributed ledger technologies. In a broader context, these terms are sometimes used interchangeably and sometimes strongly differentiated; the ideas in this paper can be applied to both at a conceptual level.

## II. THE WAVE OF CHANGE KNOWN AS BLOCKCHAIN

In light of the potential changes blockchain may bring to business and operating environments – as both an enabler and a driver – it seems prudent to consider its implications on internal control. Blockchain implementations might address, or even eliminate, extant internal control weaknesses; might be used to improve existing controls; and – particularly in the absence of recognized best practices – might pose new risks or challenges in practical contexts.

### What is blockchain?

There are many conflicting definitions of blockchain, but drawing on a variety of sources this paper uses the following working definition: *blockchain is an append-only ledger, a sequential database maintained by a decentralized network of users responsible for agreeing upon additions to the chain and secured through cryptography.*<sup>2</sup> In laymen's terms, a blockchain is a secure, transparent, irreversible digital ledger shared across participants. It is important to note that many different types of blockchains exist; there is no singular "the blockchain."

Many of the changes that proponents attribute to the adoption of blockchain are not found in isolation; it is "blockchain plus something" (i.e., other emerging technologies) that may make the changes possible. These technologies focus on supplementing or eliminating manual tasks, and moving toward a more streamlined state of financial reporting with more timely reporting of relevant information. Certain tools and technologies that may be helpful in further exploiting the potential evolution of blockchain include the following:

#### Artificial intelligence (AI)

AI is an area of computer science where intelligent machines work and react like people for tasks like decision-making, problem-solving, emulating senses, learning, planning, and activities like visual perception and speech recognition. It is particularly useful at identifying patterns and outliers. AI can be used to augment human involvement or as its replacement. For instance, AI can be used to analyze real-time trade transactional data and other information on a blockchain to simulate human judgment in classification, recording, analytics, and decision-making.

#### Internet of Things (IoT)

Internet of Things is a broad term for the growing list of things that can link to the Internet. With home automation devices, just about anything that can turn on and off can be Internet-enabled and be part of a network of things that can monitor, report about, and act upon the environment around it. IoT devices can potentially write to or act upon information in a blockchain to assist auditors in their work.

#### Big Data/Open Data

The availability of data beyond an entity's own books and records, so-called exogenous data, can facilitate broader industry analytics to provide greater context to advanced audit data analytics. Big data refers to the wide variety of data coming from sources such as IoT, social media, and other data sources too large or complex to be processed by traditional applications. Open data is a subset of big data: large, usually structured, data sets, usually made available by governments.<sup>3</sup> Big data, IoT, AI, and blockchain may all be used together in the future and, working in conjunction with internal control processes, could become a powerful toolset.



<sup>2</sup> Cryptography is relevant in that before any transaction is entered on a blockchain it must be agreed to through a consensus protocol. Each block is linked to the prior block with a unique identifier (i.e., a "hash").

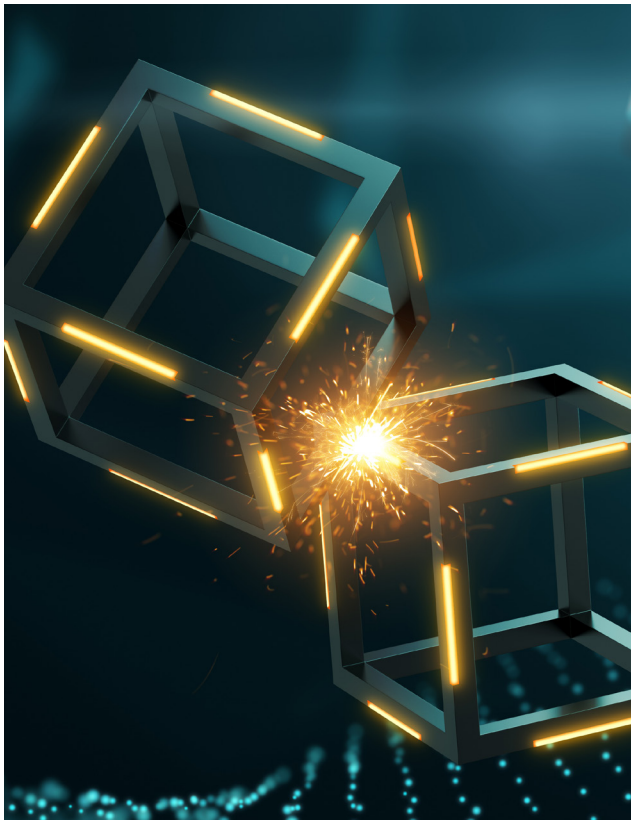
<sup>3</sup> [www.data.gov](http://www.data.gov).

### Implications for Internal Control

The internal control environment is likely to be different in a blockchain-enabled world. As such, it is important to consider and leverage these differences, factoring in blockchain capabilities, attributes, risks, and benefits. Leveraging distinctive capabilities of blockchain to enhance internal control, in turn, may promote greater:

- Effectiveness and efficiency of operations,
- Accuracy, consistency, and reliability of financial and other reporting, and
- Compliance with applicable laws and regulations.

In many ways, the control considerations with respect to implementing and operating blockchain solutions are much like those of a new Enterprise Resource Planning (ERP) or document management system. When considering financial reporting controls, certain “mainstay” financial controls (e.g., reconciliations) and processes (e.g., creation of financial reports) will likely fundamentally change. Further, new risks may emerge, which will require new controls. See sidebar for examples of how financial reporting controls and processes may change.



### EXAMPLES OF HOW FINANCIAL REPORTING CONTROLS AND PROCESSES MAY CHANGE

#### Internal controls related to the control environment

The amount of control an entity may be able to impose within different blockchain environments will vary. In many cases, control will no longer rest within the entity. This will impact how entities consider and evaluate issues within the control environment.

#### Reconciliations

With the use of a blockchain solution to respond to reconciliation-heavy areas (e.g., intercompany transactions), reconciliations will become highly streamlined, efficient, and result in increased visibility to all parties to the transaction.

#### Confirmations

With the ability to reperform calculations of transactions on the blockchain, there may no longer be a need for certain types of confirmations. However, there may also be an increased need for other confirmations with potentially new service providers.

#### Vendor and supplier approval

The use of blockchain may change the nature of an organization’s relationships with vendors and suppliers (e.g., how transactions are processed, visibility to pricing, and reporting and transparency of information).

#### Third-party service providers

Like other technology solutions, blockchain solutions may be controlled internally or sourced externally. Most externally sourced systems are typically overseen by a particular third party, the service organization. Management can request a type 2 SOC 2® system and organization controls report providing information about “the fairness of the presentation of [third party’s] management’s description of the service organization’s system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.”<sup>4</sup> Consequently, the demand for some form of SOC reporting in these environments will likely increase.

#### Decentralized external systems

In a blockchain world, there may be no singular, centralized management to oversee a particular blockchain. Although the pre-established rules (protocol) of the designers and changes brought on by the consensus of the stakeholders can be communicated, there may be no singular external entity that can be held accountable for achieving the control objectives or held responsible when there are problems. This lack of accountability poses a serious challenge. Without centralized management, there may be no simple or easy way to engage a SOC auditor and, absent SOC reports, enterprises must consider alternatives.

<sup>4</sup> [www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html](http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html).

## EXAMPLES OF HOW FINANCIAL REPORTING CONTROLS AND PROCESSES MAY CHANGE (CONT.)

### Integration of Digital Assets

Another way blockchain can be different from traditional technology solutions is integration of digital assets into the system. Some blockchains have their own integrated digital payment or value that exists nowhere else and can be tracked no other way. Traditional systems can link into banking or other financial systems; blockchain is sometimes the system itself.

### Electronic audit trail

An important benefit from certain blockchains is the automatic creation and presence of an electronic record of all transactions (i.e., an audit trail). Nevertheless, additional challenges exist with respect to determining ownership and rights, and just because a transaction is on a blockchain does not necessarily validate the transactions for books and records purposes. Further, it is possible that the evidence an auditor may wish to find is not on the chain itself (“on-chain”); although, there may be sufficient context to be able to get that information from other sources (“off-chain”), if they exist and are readily available.<sup>5</sup>

### Work of internal and external audit

Given the underlying blockchain-enabled platform for implementing internal control, the work of both external and internal auditors may be facilitated by the increased automation of controls and interactions with other emerging technologies (e.g., AI, IoT). An internal control environment facilitated by blockchain may enable a more reliable internal audit environment on which external auditors may be able to better rely. Coordination of the work performed, and coverage achieved by the external and internal auditors may be enhanced.

### Continuous real-time financial reports

More substantive and substantial continuous real-time financial reports will be possible and may become routine. Some parties may wish to have access to a blockchain and produce their own ad hoc reports (and be able to access real-time information), rather than receive agreed-upon, periodic reports from an organization.

### Monitoring becomes the only control “after the fact”

If internal environments are streamlined to the point that once a transaction hits the system, the end reporting is pre-determined, one could make the case that everything other than monitoring is considered “before the fact”/transaction pre-processing, and the only controls needed “after the fact”/post-processing are monitoring controls.

## Types of Controls in a Blockchain World

Controls are characterized as preventive (before risk materializes) and detective (during or after risk materializes). With blockchain, these control types are still relevant and applicable.

Table 3. Implications of Blockchain on Types of Controls

Type of Control	Implications of blockchain
<b>Preventive controls</b>	Recognizing the immutable nature of transactions recorded on the blockchain, there is a premium on recording transactions correctly the first time.
<b>Detective controls</b>	The visibility of transactions in a blockchain world provides new avenues for detective controls, when the necessary information is either available <b>on-chain</b> or discoverable <b>off-chain</b> from the on-chain record. In addition, because a significant amount of data will be available, blockchain coupled with the analytical abilities of other emerging technologies – such as AI, IoT, and data analytics – may be used as a means of detecting anomalies <sup>6</sup> . The challenge, in a blockchain world, is what to do when an issue is identified. Although generally corrections are still possible, given blockchain’s append-only feature, corrections will need to be reflected as adjustments rather than directly as corrections to an existing transaction. Note that this will depend on the specifics of the particular blockchain being used.

Given the speed with which transactions are processed and recorded on the blockchain, coupled with the immutability and irreversibility of such transactions, the implementation of more preventive rather than detective controls will likely

become more prevalent to assist companies in mitigating the risk of significant loss or error. Companies may also consider increasing the frequency with which detective controls are performed to promote more timely identification of errors.

<sup>5</sup> On-chain refers to information that is stored on the blockchain itself. In contrast, off-chain refers to information not stored on the blockchain, but directly or indirectly connected to the information on-chain.

<sup>6</sup> For instance, comparisons of internally and externally generated data will become quite efficient, and inconsistencies, if any, will be quickly discovered and highlighted. This will become a powerful means of monitoring. See also sidebar on page 4.

### III. COMPONENTS AND PRINCIPLES OVERVIEW

When implementing blockchain, the potential implications for ICFR, considering each COSO component and principle (see Table 4), should be analyzed. It is helpful to consider:

- Blockchain's usefulness in achieving the principles of the *2013 Framework*
- New threats or risks that may arise from blockchain implementation that impact the referenced principle
- Examples of how to mitigate those risks while seeking the greatest benefit

Table 4. *2013 Framework Control Components and Summarized Principles*

Components	Principles
Control Environment	<ol style="list-style-type: none"> <li>1. Demonstrates commitment to integrity and ethical values</li> <li>2. Exercises oversight responsibility</li> <li>3. Establishes structure, authority, and responsibility</li> <li>4. Demonstrates commitment to competence</li> <li>5. Enforces accountability</li> </ol>
Risk Assessment	<ol style="list-style-type: none"> <li>6. Specifies suitable objectives</li> <li>7. Identifies and analyzes risk</li> <li>8. Assesses fraud risk</li> <li>9. Identifies and analyzes significant change</li> </ol>
Control Activities	<ol style="list-style-type: none"> <li>10. Selects and develops control activities</li> <li>11. Selects and develops general controls over technology</li> <li>12. Deploys control activities through policies and procedures</li> </ol>
Information and Communication	<ol style="list-style-type: none"> <li>13. Uses relevant, quality information</li> <li>14. Communicates internally</li> <li>15. Communicates externally</li> </ol>
Monitoring Activities	<ol style="list-style-type: none"> <li>16. Conducts ongoing and/or separate evaluations</li> <li>17. Evaluates and communicates deficiencies</li> </ol>

The internal control opportunities and risks associated with blockchain will vary based on the nature and type of blockchain implemented and the amount of influence, oversight and control an organization can impose within different blockchain environments. In applying the *2013 Framework* to blockchain, it is important to be aware of the following:

- Implementing a **private, permissioned blockchain** within a single enterprise will bring some new considerations and risks, but will also be an experience much like adopting any previous technology, if management has the ability to control the blockchain, including the inputs, processing, and outputs.
- Joining a **consortium blockchain** or another organization's private blockchain brings new inter-organizational challenges such as risks and controls being shared across organizations, demanding more coordinated decision-making.
- Making a **public, permissionless blockchain** part of the financial reporting environment brings an entirely different set of risks and challenges, because decision-making may be decentralized, leaving little room for individual influence and little individual accountability. While this may be compared with the use of an outside service organization, management will need to take a much broader and potentially more in-depth view of these "outsourced" processes.



## Control Environment

Summary	Principle
1. Demonstrates commitment to integrity and ethical values	The organization demonstrates a commitment to integrity and ethical values.
2. Exercises oversight responsibility	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Establishes structure, authority, and responsibility	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. Demonstrates commitment to competence	The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. Enforces accountability	The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Control Environment is primarily about the existence of a risk and control-conscious culture and the policies, processes, and structures that guide people at all levels in carrying out their responsibilities in a manner that is consistent with the entity's commitment to integrity and ethical values. The perception of blockchain as just another (albeit exciting and perhaps revolutionary) technology could result in underestimating its potential impact on the control environment. Blockchain does not change human nature or the behavioral aspects of governance that have a significant influence on the overall control environment – those remain largely unchanged regardless of the technology used.

Nevertheless, there are important control environment implications when using blockchain. It is important that management has the appropriate skill set to sufficiently understand how the entity plans to use the blockchain and the governance structure of the particular blockchain (i.e., the unique governance structure and ongoing health and operating effectiveness of such structure), in order to assess whether the use of blockchain supports the entity's commitment to integrity and ethical values. It is also important that the board of directors has a sufficient understanding of the technology to fulfill their oversight responsibilities.

### Using Blockchain to Enhance the Control Environment

- Blockchain can provide organizations with a method of executing and recording transactions with minimal human intervention. Further, the highly automated nature of blockchain, coupled with the technology's ability to validate and record immutable transactions on a shared ledger, provides organizations with opportunities to avoid human error and combat transactional and reporting fraud.

- With blockchain, processes will commonly have cryptographically verifiable **immutability** and irreversibility; thus, with a well-designed and implemented blockchain, management should be able to rely upon and provide evidence of actions.
- The increased visibility provided by a shared ledger system contributes to transparency, which promotes a strong control environment and facilitates the ability to provide real-time financial reports.
- Blockchain, coupled with the analytical abilities of other emerging technologies such as AI and data analytics, may allow organizations to identify deviations from an organization's standards of conduct on a timelier basis. This may prove especially helpful in implementing effective oversight in large and/or decentralized organizations.
- In some instances, blockchain may facilitate the removal of management's manual intervention from processes, making them largely immune to the influence of management decisions, integrity, and ethics.

### New Threats or Risks Posed by the Use of Blockchain

- The pseudo-anonymity<sup>7</sup> of the parties that transact on a blockchain, coupled with the open nature and potential lack of guard rails, poses a threat that a permissionless blockchain may be used for unethical exploits.<sup>8</sup>
- Each blockchain is set up with a unique governance structure that needs to be actively monitored concerning the health and the operating effectiveness thereof.

<sup>7</sup> In a public blockchain, assets are exchanged between blockchain addresses and private keys are used for authorization, but people and organization names are not explicitly associated with those addresses and keys. This offers a level of disguised identity, because it is possible to transact without giving any personally identifiable information. It is, however, possible to pierce the veil of identity through various de-anonymizing methods.

<sup>8</sup> Recognizing that while efforts are underway to incorporate the Legal Entity Identifier (LEI, a unique serial number for organizations globally) into blockchain – which would make assessing conflicts of interest easier to identify and assess – there still is a threat of potential unethical exploits in the current space given the pseudo-anonymity.

For certain blockchains, the decentralization and lack of a central intermediary, system or oversight body to hold parties accountable for their actions leads to situations in which there is literally “no one minding the store.” If and when things go wrong, for certain blockchains, there is no recourse to anyone, and thus no accountability – a serious governance-related drawback.

- Although generally, the use of blockchain is considered forward-thinking and positive, the act of advocating, adopting, and embracing blockchain or associating with certain groups may be seen negatively by an organization’s employees, clients, advisors, and overseers. Further, depending on the nature of the blockchain and the fellow participants in the blockchain, an organization may face reputational risk, because participating may be perceived as sharing in the lowest common denominator of the group’s ethics (i.e., reputation by association). For certain arrangements, controlling who gets in and **consensus** changes to the system will be out of the control of management.
- Blockchain’s newness and complexity means competent personnel are hard to find, and a commitment to competence is difficult to guarantee or assess. The potential that blockchain has to facilitate pervasive automation means more tasks can be done automatically, and the nature of people’s responsibilities and related competencies can change, sometimes dramatically. Similarly, it may be difficult for management and those charged with governance to obtain the relevant level of understanding and expertise to effectively oversee the implementation and use of blockchain.

### Mitigating New Threats and Risks Associated with Blockchain Implementation

In response to the specific risks identified, management and the board of directors may consider the following actions:

- Where applicable, develop a code of conduct that governs the conduct of parties within a blockchain and establishes guidelines for addressing noncompliance. Organizations seeking to implement a private blockchain or create a consortium blockchain may develop such a code of conduct and mechanisms to (1) validate each member’s commitment to ethics and integrity and (2) enforce accountability with the code of conduct and report/address/remediate any deviations. Organizations should have a clear understanding of the governance process

and actively monitor and evaluate whether it is effective. Organizations may also consider engaging an independent external party to provide oversight and validate adherence to the established code of conduct, if possible. In such cases, it will be important for the organization to have clear reporting lines established to ensure the external party reports directly to those charged with governance of each respective party.<sup>9</sup>

- Also, consider expectations regarding the code of conduct, responsibilities, and authority of outsourced service providers. Although much of the activity related to outsourced service providers occurs outside the blockchain, the results could be challenging if unreliable data associated with these relationships enters the blockchain.
- Develop due diligence policies that establish guidelines and criteria for determining parties with whom the organization will transact; parties with whom the organization will grant access to a blockchain; and the public blockchains that an organization may elect to use in conducting transactions. These policies may include Know-Your-Customer (KYC) procedures, Anti-Money Laundering (AML) procedures, asking for SOC reports, and other due-diligence procedures to understand the identity and integrity of the counterparty. Such procedures may also include obtaining an understanding of the policies in place to govern the conduct of parties within a blockchain. Maintaining an understanding of the governance process and continuing to monitor its effectiveness is particularly important.
- Assess the need to obtain or build expertise surrounding the blockchain technology, to ensure effective implementation of blockchain and appropriate use and updating of the technology post-implementation. Further, such competencies should continue to be re-evaluated and monitored as the technology continues to evolve rapidly.
- Ensure that the organization is capable of assessing and evaluating the new technology and process. This may be achieved through in-house resources, outsourced resources, or a combination.

<sup>9</sup> Establishing a code of conduct will most likely not be feasible for public blockchains. As such, management and those charged with governance will need to evaluate the risks associated with using a public blockchain and their corresponding levels of tolerance for such risks.

- Establish cross-disciplinary teams, which include blockchain specialists and representatives from each aspect of the business that are affected by the implementation of the technology (e.g., IT, accounting, finance, operations, and internal audit). Such teams should be engaged throughout the planning, development, and implementation process.
- Evaluate and enhance, if needed, the board and audit committee’s ability to understand the potential uses and risks associated with blockchain and its ability to effectively oversee the implementation and use of blockchain.
- Define degrees or levels of responsibility and authority surrounding the blockchain technology, considering segregation of duties concerns (e.g. access-level privileges, **private key** access and the ability to authorize transactions, and associated financial reporting). Develop a suitable succession plan for assigned degrees or levels of authority and responsibility surrounding the blockchain that are key to internal controls.
- Establish clear reporting lines for consortium or private blockchains that identify individuals or a group of individuals responsible for handling disputes which arise among members of a network, if not built into the underlying protocol. This could involve defining a dispute resolution jurisdiction and mutually agreed-upon procedures as well as potential parting of ways when “irreconcilable differences” arise.

### Risk Assessment

Summary	Principle
6. Specifies suitable objectives	The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. Identifies and analyzes risk	The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. Assesses fraud risk	The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. Identifies and analyzes significant change	The organization identifies and assesses changes that could significantly impact the system of internal control.

Risk assessment involves the iterative process of identifying and assessing threats to the achievement of objectives. Blockchain will likely bring about new objectives and risks that need to be addressed. It is important for organizations to have the appropriate skills and resources to comprehend the unique risks associated with blockchain and identify, assess, and address those risks on an ongoing basis.

#### Using Blockchain to Enhance Risk Assessment

- The integration of blockchain with other emerging technologies could provide management, the board, and external parties with real-time reporting – thereby creating a more agile business environment – that identifies and assesses the achievement of various entity objectives (e.g., operational, external financial reporting, compliance or other internal objectives).





## New Threats or Risks Posed by the use of Blockchain

- Traditional risk assessments have been entity-focused, but with the use of blockchain, companies will need to consider risks more broadly. For example, entities may consider the susceptibility of the other parties within the blockchain network to risk and the effects that this could have on their respective businesses. Furthermore, different risk appetite/risk tolerances among members of a blockchain can lead to conflict when monitoring controls are designed for a blockchain. For particular blockchains, there may be questions about who is responsible for managing risks if no one party is in charge, and how proper accountability is to be achieved.
- The implementation of a blockchain may leave companies vulnerable to new fraud schemes or new avenues to carry out traditional fraud schemes. See right sidebar for examples.
- The amount of data available in a blockchain-enabled environment can become unmanageably large; attempting to manage too much data may bring about data overload, resulting in exacerbated data governance issues.
- **Smart contracts** are both a potential risk and an important part of the risk mitigation tool set. Once put in place, they will self-execute and are difficult to stop. Therefore, if developed incorrectly or manipulated, the effects could lead to error or potentially significant loss on a magnified scale.
- The use of a blockchain could present issues surrounding obtaining sufficient appropriate evidence to support transactions recorded in an organization's financial records (i.e., due to the loss of the transaction audit trail in an electronic environment).
- **Digital assets** introduce a new class of assets for which there exists little or no prior experience and few meaningful parallels in managing risk and identifying unusual behavior. Businesses considering holding digital assets have incremental considerations regarding the assets themselves, including the market volatility, or lack of market for certain digital assets, cybersecurity risks around the protection of the private keys, accounting and financial reporting of such assets, and evolving regulatory requirements.

## EXAMPLES OF NEW TYPES OF FRAUD SCHEMES

- The reliability of financial information stored on the digital shared ledger is dependent on the underlying technology. If the underlying consensus mechanism, or other aspects of the blockchain, have been tampered with, this could render the financial information stored in the ledger to be inaccurate and unreliable.
- The pseudo-anonymity of parties on a blockchain can increase opportunities for collusion or obfuscate related party transactions. This risk may be more applicable with reference to public blockchains, given the likelihood of a more pseudo-anonymous environment with large numbers of unknown parties on such networks.
- Although a reliable blockchain provides transaction security, it does not provide account/wallet security; hence, value stored in any account is still susceptible to account takeover, if an organization's private keys are stolen or compromised.
- There are heightened cybersecurity risks to blockchain. If the underlying technology is compromised as a result of cyberattacks an organization's assets could be stolen. Furthermore, the impact of cyberattacks could extend beyond the organization to others within the network. There are also some unique aspects of cyber risks affecting blockchain as a result of its use of cryptography, wallets, and its decentralized nature.

<sup>10</sup> Deloitte's 2019 Global Blockchain Survey, *Blockchain Gets Down to Business*. Deloitte Insights.

- Integration challenges between the blockchain and existing legacy systems may arise. Blockchain will most likely be a tool that is a part of a larger core infrastructure and will have to work seamlessly with legacy infrastructure. Poor integration of blockchain with other entity systems could result in less-than-desired outcomes, such as poor client experience and regulatory noncompliance issues. See sidebar at right for additional discussion.
- The regulatory environment surrounding blockchain, smart contracts, and digital assets continues to evolve and may vary across jurisdictions, leading to uncertainty around the regulatory requirements (including tax, data privacy, and protection, reporting, or other regulatory requirements).
- The blockchain business environment also continues to evolve, with improvements in the technology, best practices, and new use cases being identified every day. The ability to monitor the fast-paced, and rapidly evolving, environment may prove difficult and challenging.
- Fragmented solutions that exist today may soon be replaced. The significant investment of time, talent, money, and media coverage into the technology and methodology has resulted in a highly fragmented market of solutions, with overlapping capabilities and little interoperability. Given the ongoing haphazard, uncoordinated approach to blockchain development, Gartner has predicted that 90% of 2019's blockchain implementations will require replacement by 2021.<sup>11</sup>

In addition, due to the highly automated nature of the technology, general IT and other risks may be exacerbated or heightened in a blockchain environment, such as in the following areas:

- Although issues such as access rights to the system and data and program integrity are common to other technological solutions, concerns about technology access rights are heightened because the effects of inappropriate access issues can become shared issues across companies on a blockchain.

### Interoperability of Blockchain

There are limited success stories related to blockchain interoperability despite indications that businesses believe the integration of multiple chains is important.<sup>10</sup> In an era where the Web has brought platform agnosticism, and Macs, PCs, and portable devices can all access important resources, most blockchain use today is stand-alone. Future uses will have to be interoperable, as value networks exchange information with service networks, which exchange information with content networks, and all work together with AI or IoT or traditional databases and systems. The market has proven the network effect in the past: adoption begets more adoption and enhancements, which will in turn breed more adoption, and so on.

- Where the blockchain is visible to many parties, the visibility may bring cybersecurity challenges and cyberattacks.
- For most public blockchains, users may not be able to obtain an understanding of the general IT controls implemented and the effectiveness of these controls. Furthermore, where there is no central authority to administer and enforce protocol amendments, there could be a challenge to establishing development/maintenance process control activities for the technology.
- Given the speed with which transactions are recorded on a blockchain, coupled with the immutability and irreversibility of transactions, organizations may face increased risk of significant loss or error in the event that deficiencies in internal controls over a blockchain are not identified and corrected in a timely manner. Additionally, the elimination of centralized overseers and intermediaries may leave companies with no recourse when errors or losses occur, creating governance challenges. Companies engaging in blockchain-based transactions cannot rely on central intermediaries, such as a bank, to restore their funds in the event of fraud. As such, companies will need to consider whether enhancements to their internal control infrastructure may be warranted.

<sup>11</sup> [www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain](http://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain).

- As organizations begin to incorporate blockchains, there will be a transition period. During this time, legacy systems, ERPs, or third-party cloud-based systems will perform front-end processing and data collection, then interface with a blockchain for additional processing or recording. Although data is largely secure and tamper-proof once in a blockchain, that data is still vulnerable to common IT risks while outside the blockchain.<sup>12</sup> The interface transmission of data from upstream systems to a blockchain will be a sensitive control point in these new environments.

### Mitigating New Threats and Risks Associated with Blockchain Implementation

In response to the specific risks identified, organizations may need to consider some of the following actions:

- Establish objectives for the use of blockchain such that its implementation supports reliable and verifiable books and records to enable appropriate accounting and effective financial reporting.
- Develop more robust risk assessment processes that consider the implications of blockchain on all aspects of the organization. In developing such an assessment, it may be helpful for companies to engage relevant IT and blockchain specialists to assist in identifying potential threats, areas of risk, and fraud schemes (based on knowledge of the organization's control environment, the blockchain, and common fraud schemes). Performance of such a risk assessment process prior to the implementation of blockchain will also be helpful in evaluating the potential benefits and costs associated with the technology.
- Develop procedures to stay abreast of changes in the business and regulatory environment around blockchain. Early engagement of the entity's legal counsel and internal audit department in the implementation of the technology may assist in keeping informed about changes in the regulatory environment.
- As blockchain is integrated into an organization's business information process, and such integration has financial

reporting implications, management should engage with appropriate parties (e.g., internal auditors, external auditors) to identify new risks relevant to financial reporting, internal control, appropriate accounting treatment, and implications for audits (e.g., potential auditability challenges).

- Engage appropriate IT and blockchain specialists with knowledge of the entity's existing systems to assess how blockchain will be integrated into and operate as a part of the entity's existing IT infrastructure, prior to its implementation.
- Develop strong governance and change-control processes to deploy new or amend existing smart contracts or changes to the blockchain. Such processes should also contemplate incident response management, and methods to identify and respond to glitches in smart contract and blockchain operations.

While control activities will be discussed more fully in the next section, example controls to mitigate fraud and cybersecurity risks could include:

- Implementing appropriate segregation of duties between the ability to authorize blockchain transactions (i.e., access to the private keys) and the ability to record transactions within the entity's general ledger, as well as establishing appropriate access controls surrounding the ability to authorize and execute changes to the underlying technology.
  - User-acceptance testing should be undertaken through blockchain prototypes and realistic use cases to avoid undesirable outcomes, including with respect to segregation of duties.
- Establishing controls over information transfer to and from the blockchain to the entity's general ledger system and other off-chain systems.
- Using multisignature or key sharding techniques<sup>13</sup> to manage the ability to authorize blockchain-based transactions.

<sup>12</sup> M.D. Sheldon, "A Primer for Information Technology General Control Considerations on a Private and Permissioned Blockchain Audit," *Current Issues in Auditing*, Vol. 13, No. 1, (Spring 2019): A15-A29.

<sup>13</sup> Key sharding, like multisignatures, is a method of managing keys to decentralize risk and control by requiring multiple parties to be involved (e.g., by splitting up portions of the private key).



- Deploying a combination of preventive controls and detective controls to protect from intruders accessing the information systems; or when an intrusion has occurred, quickly detecting and preventing further access after the initial layers of defense are compromised.
- Developing and implementing a structured approach to manage the identification and assessment of cybersecurity risk, including an assessment of how the organization and other members of the blockchain network may identify and address shared cybersecurity risks.

## Control Activities

Summary	Principle
10. Selects and develops control activities	The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. Selects and develops general controls over technology	The organization selects and develops general control activities over technology to support the achievement of objectives.
12. Deploys through policies and procedures	The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Control activities help mitigate risks to the achievement of objectives and are performed at all levels of the organization, at various stages within business processes, and over the technology environment. Control activities may be preventive or detective in nature and may encompass a range of manual and automated activities, such as authorizations and approvals, verifications, reconciliations, or business performance reviews. The goal of control activities is to sufficiently mitigate risks to the achievement of objectives to acceptably low levels.

Blockchain – with its use of cryptographic methods, capability to create smart contracts, and its ability to provide increased visibility – can be an important adjunct to enabling control activities, making such controls more reliable and secure, and providing enhanced or new tools to carry out the necessary steps in this context. At the same time, new challenges emerge requiring specialized considerations for control activities and for IT general controls.

### Using Blockchain to Enhance Control Activities

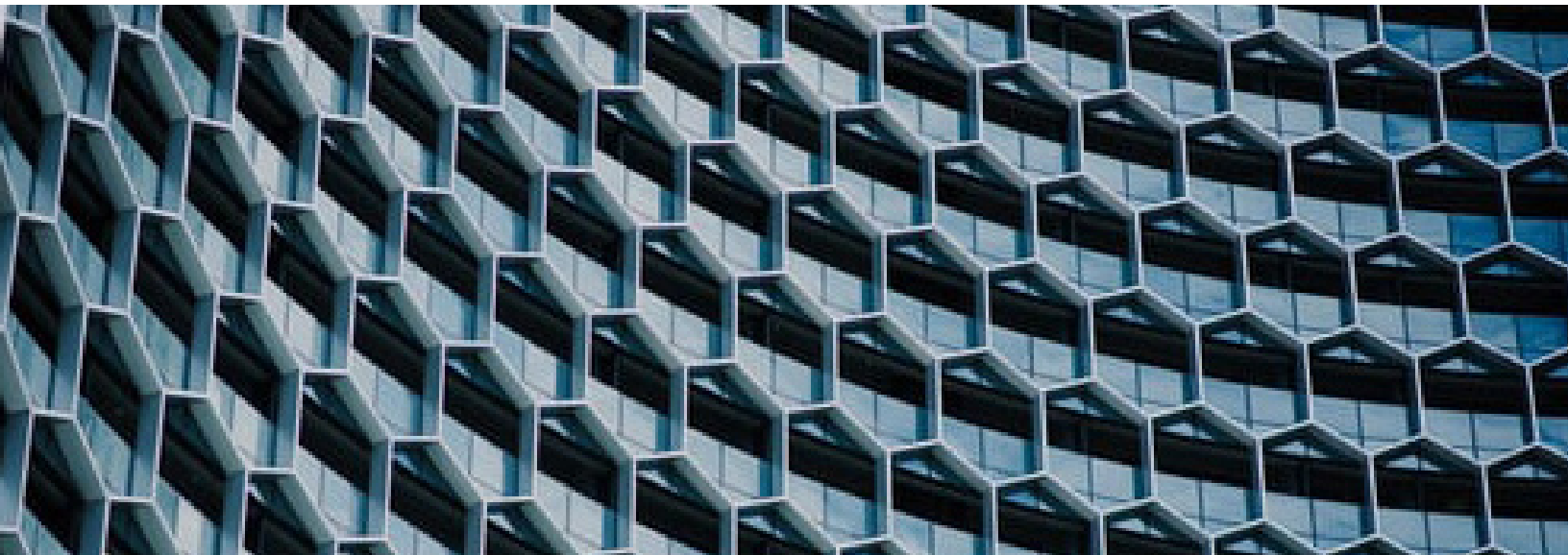
- A well-designed and implemented blockchain may provide companies with the ability to further enhance their internal controls (e.g., by promoting accountability, maintaining record integrity, and being irrefutable). A properly implemented blockchain may reduce concern over direct access to record, modify, or delete historical data. For example, for certain blockchains, once a block is sufficiently buried (i.e., newer verified blocks exist on top of it), there is minimal risk of changes to historical data unless the governing parties agree to perform a change or the chain is **forked** (presuming no breaches to the security of the blockchain).
- The highly automated nature of blockchain, coupled with the technology's ability to validate and record immutable transactions on a shared ledger, provides companies with opportunities to combat transactional and reporting fraud, due to the reduction of human intervention in the financial reporting process. With the use of blockchain, traditional opportunities to commit fraud or manual error will decrease, thereby reducing risk of loss. Further, the fact that multiple members participate in the consensus protocol allows for greater likelihood of errors being identified as many parties validate the accuracy of the transaction prior to posting.
- Blockchain eliminates the need for certain IT general controls as it minimizes the risk of data loss and therefore, traditional controls like data backups, batch processing among **nodes**, and disaster recovery may not be necessary, unless a platform is abandoned or goes into disuse. As the blockchain ledger is shared across multiple nodes on the network, reliance on backups is less important because the most recent versions of the ledger may be recovered from other non-affected nodes across the network.
- Use of blockchain may also mitigate the risk of untimely transaction processing and recording, because depending on the particular blockchain, it may provide the organization with the ability to process and record transactions on a near real-time basis. This capability can greatly reduce errors.

- Smart contracts may enhance control activities and prevent opportunities for fraud (due to the automation of executing contractual terms). Note, however, that as smart contracts are a tool, the tool or inputs used by smart contracts (including inputs from blockchain **oracles**) could be manipulated to commit fraud.

### New Threats or Risks Posed by the use of Blockchain

- The appropriate functionality of blockchain is highly dependent upon the reliability of the underlying technology and the implementation of complementary business process and general IT controls. A poorly implemented blockchain or the lack of appropriate supporting controls could result in new or more widespread issues related to blockchain, including issues surrounding smart contracts, key management, consensus protocols, chain **rollbacks**, and forks.
  - Smart contracts are powerful but can add complexity. Like any other programming application, smart contracts may contain programming errors or back doors, or be subject to other challenges. Poorly designed and implemented smart contracts with deficient business logic could lead to large-scale automatic execution and recording of invalid transactions, for which there could potentially be no recourse – a highly undesirable outcome.
  - Blockchain does not provide management protection over access to an organization's private keys and hence does not provide direct control of its digital assets. A lack of proper controls over the private keys and the ability to initiate blockchain-based transactions could lead to potential loss or misappropriation of organization assets.
- Enterprise key management software is only beginning to emerge, as are key management guidelines.<sup>14</sup>
  - The consensus protocol (or mechanism) of a blockchain sets the rules, preconditions, and requirements for validating transactions in accordance with the agreed-upon rules. A poorly designed and implemented consensus protocol compromises the technology's ability to properly validate transactions in accordance with the agreed-upon rules. In such cases, information recorded on the shared ledger may be invalid and unreliable. Even with the implementation of an effective consensus protocol, there is still a risk that transactions recorded on the blockchain may be invalid, for many reasons, including if the distribution of computational power among members of the network is such that one or more members of a group of members is able to manipulate the consensus protocol, a.k.a., a "51% attack".
  - Consensus protocols drive updates and changes to the system. Chain rollbacks are a primary method of "correcting" major errors in a blockchain but can be used to circumvent the immutability of a chain through restarting from an earlier point. As such, chain rollbacks may provide management with the ability to alter transactions recorded on the blockchain.
  - The completeness of transactions recorded on the blockchain may be brought into question if the organization engages in recording off-chain transactions. Off-chain transactions are not captured on the blockchain and would require additional considerations and controls to reconcile with on-chain transactions and the associated financial reporting.

<sup>14</sup> NIST Key Management Guidelines.



## Mitigating the New Threats and Risks Associated with Blockchain Implementation

### Controls over Key Aspects of the Blockchain

Although the implementation of blockchain could either enhance or impair the effectiveness of an entity's control activities, there are specific steps that can be taken to mitigate these risks and utilize blockchain to its full

potential. For example, revised policies and procedures should address new risks, internal controls, and accounting related to the use of blockchain, as well as establish responsibility and accountability for executing the policies and procedures. In addition, organizations should consider identifying and implementing relevant controls over key aspects of the blockchain, including, as appropriate, those outlined in the following table:

Table 5. Controls Over Key Aspects of Blockchain

Aspect of the Blockchain	Control Activity Considerations
<b>Nodes</b>	<p>Each computer on a blockchain network is known as a “node.” It will be important for companies to have established controls governing the activities of nodes that store copies of the database, perform validation of transactions, work to prepare data to be added to the chain, or perform other services. Controls may relate to the following objectives:</p> <ul style="list-style-type: none"> <li>• Making sure there are enough nodes working to minimize the opportunity for some to collaborate to attack the system. Ensuring the computational power is appropriately distributed across all nodes, such that the consensus protocol cannot be manipulated.</li> <li>• Testing the availability of blockchain data from different nodes in the network.</li> <li>• Verifying the consistency of data obtained from different nodes in the network.</li> <li>• Testing that nodes are performing relevant validations before agreeing to add data to the chain.</li> <li>• Tracking and providing incentives for correct validations and penalties for incorrect validations.</li> </ul> <p>(Note: An organization may not be able to perform these in relation to a public blockchain, given the large number of nodes operating on the network.)</p>
<b>Consensus Protocols</b>	<p>Consensus protocols for specific blockchains should be periodically evaluated to determine whether:</p> <ul style="list-style-type: none"> <li>• The appropriate nodes are authorized to participate in consensus.</li> <li>• Protocols have been appropriately designed and are operating effectively.</li> <li>• Incentives for complying with the protocols and penalties for not complying have been appropriately designed to mitigate fraud.</li> </ul> <p>The major categories of consensus include proof-of-work, proof-of-stake, or majority vote.<sup>15</sup></p>
<b>Private Keys</b>	<p>Companies should take steps to manage access to their private keys. These controls will be dependent on how such keys are stored (e.g., hot <b>wallet</b> or cold wallet). In some instances, companies may engage a third-party custodian to assist in key management or to manage the assets directly. Custodians may require splitting access to the private key across multiple parties, thereby requiring approval of transactions by multiple parties (multisignature). It will also be important to ensure that the organization has considered appropriate segregation of duties to ensure that persons who approve blockchain transactions do not have the ability to record transactions within the organization's books and records.</p>
<b>Smart Contract</b>	<p>To mitigate the risks associated with smart contracts companies may:</p> <ul style="list-style-type: none"> <li>• Implement controls to validate the appropriateness of the design and implementation effectiveness of smart contracts, track changes and updates in a controlled fashion, and ensure there is proper documentation and historical record to establish accountability.</li> <li>• Implement controls over the inputs into smart contracts, including inputs from blockchain oracles.</li> </ul> <p>Controls over smart contracts should provide timely alerts and exception reports to ensure that everything is working as intended and departures and deviations are promptly reported to appropriate parties.</p>

<sup>15</sup> More information on the nature of public and private blockchains is available in the posting by one of the founders of Ethereum, Vitalik Buterin, “On Public and Private Blockchains,” Buterin, V. 2015. Available at <https://ethereum.github.io/blog/2015/08/07/on-public-and-private-blockchains/>.

Information and Communication	
Summary	Principle
13. Uses relevant, quality information	The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
14. Communicates internally	The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. Communicates externally	The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

The Information and Communication component of the *2013 Framework* focuses on identifying, processing, and communicating relevant information to and from internal parties and external parties. Blockchain has the opportunity to support the effective and timely communication of information by connecting organizations for collaboration, while also presenting new risks and threats. At the same time, organizations must consider the information and communication changes expected to be needed in light of the use of blockchain. For example, most blockchain implementations today do not include on-chain all of the information helpful to support management's representations about classes of transactions, events, or account balances.

#### Using Blockchain to Promote Information and Communication

- Blockchain results in enhanced visibility of transactions and new avenues for management to communicate financial information to key stakeholders (e.g., through ad hoc, real-time financial reporting).
- As a comprehensive, shared database, blockchain can be a foundation for providing data about transactions, relevant to both financial reporting and decision-making.
- Blockchain, if properly implemented, can promote the availability of data that is accessible, accurate, consistent, current, retained, and timely.
- Data is less likely to be lost when being entered into or aggregated within a common and comprehensive digital ledger, promoting better visibility and offering supplemental provenance evidence.

#### New Threats or Risks Posed by the use of Blockchain

- With the uncertainty about the full capabilities of blockchain and what blockchain is and does, there can be a false sense of comfort that information on a blockchain is always correct, information is available, people have been notified, and feedback has been received. In fact, information on a blockchain only maintains the integrity of what was entered; as in everything else, "garbage in, garbage out" prevails. Furthermore, the reliability of the data stored on a blockchain is dependent on the effectiveness of the underlying technology. Blockchain supported by flawed technology may provide data that is unreliable and cannot cure underlying deficiencies.
- Although blockchain has the ability to record large amounts of transactional data in a timely manner, this data will need to be processed into useful and actionable information.
- As it pertains to financial reporting, companies may face challenges gathering sufficient appropriate evidence to support assertions they make about the digital assets or digital asset transactions processed on a blockchain. Furthermore, companies may face challenges with the ability of auditors to obtain the evidence they need to assess whether the books and records are adequately supported (See Appendix 3 for further discussion of assertions.)

### Mitigating the New Threats or Risks Associated with Blockchain Implementation

In response to the new risks and threats to providing and receiving information, organizations may need to consider some of the following actions:

- Educate key stakeholders (including those charged with governance) on how blockchain will be used by the business and the associated benefits and risks of using the technology. It will be important for stakeholders to understand that although blockchain has been designed to improve the transaction execution and recording process with the aim of providing real-time validated transactions, there are still risks associated that could render the data unreliable.
- Determine that the board of directors and audit committee have the information they need to perform their related oversight responsibilities.
- Establish a method for members of a blockchain network to report any concerns. The methods may include a whistleblower hotline, if not already in place.
- Develop communication methods to ensure that operational and other changes/updates relating to the use of blockchain are communicated to appropriate personnel so they can understand and carry out their internal control related responsibilities.
- Determine new information requirements needed in light of the use of blockchain in order to produce relevant, quality information to support the functioning of internal controls.
- Develop data analytics procedures to identify and obtain relevant, quality data from the blockchain that can then be processed into information to be used to support management’s business processes and reporting objectives.
- Engage in discussions with both internal and external auditors during the development of or identification of a blockchain to be used in the entity’s processes. As a part of these discussions, it will be important for management to understand typical auditability issues associated with using blockchain and corresponding processes that can be implemented to mitigate against such issues, so that the appropriate information and support for transactions is available.

### Monitoring Activities

Summary	Principle
16. Conducts ongoing and/or separate evaluations	The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. Evaluates and communicates deficiencies	The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Monitoring controls are used to determine whether internal control, including each of the components and principles, are effective and functioning. Findings are evaluated and communicated appropriately. Blockchain does not change the need to evaluate whether the components and principles are present and functioning, but the method of evaluation may change in light of the use of blockchain (for example, when the internal control environment is shared across multiple enterprises and may require more collaboration between organizations).

### Using Blockchain to Enhance Monitoring

- As blockchain facilitates a more integrated, flow-through environment with minimized human intervention, evaluations themselves can be built into a blockchain-enabled process using smart contracts, AI, and standardized rules engines. In addition, blockchain can be used with other technologies to help in identifying information for effective oversight. For example, IoT devices can act where human intervention was previously impractical, to permit real-time recording of transactions<sup>16</sup> based on changes in the environment. Blockchain can maintain detailed data that can be summarized in different ways to allow for the completion of evaluations of varying scopes and frequencies.

<sup>16</sup> For example, IoT sensors in a shipping container can monitor for possible damage from rough movement or temperature variations and trigger appropriate claims for insurance or other contractual reparations.



- As information is collected or aggregated onto a blockchain on a real-time basis, monitoring activities can catch problems closer to the occurrence of a deficiency, minimizing exposure and speeding remediation.
- If effectively implemented, the use of blockchain may allow for more timely identification of errors and performance reviews, carried out more holistically. Advanced analytics, AI, and other tools can be used to analyze the detail allowing management to concentrate on higher risk areas. Separate evaluations performed by internal auditors can also focus on the information most relevant to their own use.
- Using ongoing evaluations to identify changes and updates to the technology, and to validate whether the components of internal control are present and functioning.
- Identifying and obtaining talent with requisite knowledge of an entity's baseline control environment, blockchain technology, and best practices surrounding monitoring techniques to 1) assist in designing and implementing appropriate monitoring controls and 2) assess the results and efficiency of such monitoring activities.

### New Threats and Risks Posed by the use of Blockchain

- Working with large amounts of data that is frequently updated could potentially exacerbate the level of, and susceptibility to, risks related to information overload and result in additional challenges in adequate monitoring.
- Similar to challenges identified surrounding the control environment component, finding competent people to design and perform effective monitoring controls over blockchain may prove challenging.
- The use cases for blockchain are growing in number and complexity, as are the regulations and laws surrounding blockchain. It is difficult to stay abreast of ongoing change and ensure proper and timely updates to the technology and to any other procedural or operational processes that are needed, including with respect to monitoring.
- The decentralization and lack of a central intermediary associated with certain blockchains may result in no established party or body responsible for executing monitoring controls, posing governance challenges.
- Assessing the unique aspects of blockchain such as consensus protocols, smart contracts, and private keys, as well as factors relating to the ongoing health, governance, and overall reliability of the blockchain in use.
- Within a consortium or private blockchain, identifying individuals who will be charged with executing monitoring controls and establishing agreed-upon policies and procedures for communicating deficiencies and taking corrective action in the event that deficiencies are identified.<sup>17</sup>
- In some instances, retaining an objective third party to assess consortium blockchains. For example, if proprietary information is needed from individual entities to determine whether the components are functioning, to evaluate deficiencies, and to communicate deficiencies, a trusted intermediary can access such information.
- Monitoring service-level agreements with and control reports from outsourced service providers. As stated earlier, if unreliable data associated with these relationships enters the blockchain, the results could be severely compromised, even catastrophically.

### Mitigate the New Threats and Risks Associated with Blockchain Implementation

In response to the new risks and threats, organizations may need to consider the following:

- Given the large volume of data processed on the blockchain and the high frequency at which these transactions are processed, using computerized continuous monitoring techniques to perform ongoing evaluations, as opposed to traditional manual techniques.

<sup>17</sup> Establishing monitoring controls over a public blockchain may not be possible given the level of decentralization and management's lack of control over the management and oversight of the technology.

## CONCLUSION AND NEXT STEPS

Many businesses, industries, and governments are investing in and exploring how blockchain could positively impact the achievement of their objectives.<sup>18</sup> When an organization evaluates the potential use of blockchain through a COSO lens, it enables the board of directors and senior executives to better understand the context and make more informed assessments of the technology's potential and applicability with respect to internal control. This enables others within the organization to perform a detailed risk analysis and in turn, develop appropriate controls to address such risks, which will facilitate the effective adoption and use of blockchain.

Many challenges need to be addressed to leverage the potential of blockchain. These challenges and issues will

likely be sorted out by organizations 1) with motivation to have transparent and accessible blockchain-based systems and 2) in industries that are being disrupted by blockchain.<sup>19</sup> These organizations bear a greater burden in identifying solutions, lighting a new path that will help other blockchain adopters in the future. Further, it is these organizations that will develop new use cases, not only advancing their own organization, but also helping others (including regulators and other stakeholders) understand the potential benefits of blockchain.

The introduction provided a list of potential stakeholders and the intended use for the document. The following table provides potential next steps for the same stakeholders.

Table 6. Next Steps for Key Stakeholders

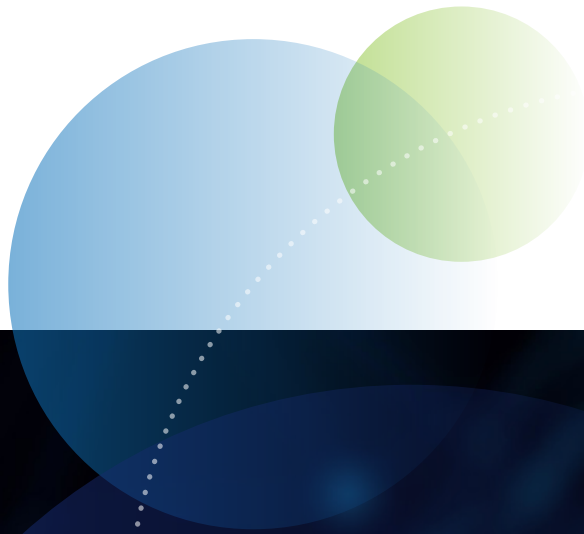
Audience	Next steps
Board of directors	<ul style="list-style-type: none"> <li>Leverage this document and relevant blockchain-related information, educational materials, webcasts, training sessions and other resources to gain a foundational understanding of the technology</li> <li>Build internal expertise on the board and support discussion at the leadership level on blockchain activities within the organization and the potential benefits and challenges</li> <li>Understand how blockchain-enabled processes may promote or reduce reporting efficiency and risk</li> <li>Understand how internal and external auditors may be considering the technology's potential</li> </ul>
Audit committee members	
Executives (CEO, CFO, Controllers)	<ul style="list-style-type: none"> <li>Build internal expertise and support discussion at the divisional and/or departmental level on the potential benefits and challenges of blockchain</li> <li>Gain insights about how blockchain is being used by peer organizations and what innovative practices are in use</li> <li>Coordinate with blockchain developers to help them prioritize and design blockchain technology that is ready for internal control</li> <li>Talk with external auditors to understand how blockchain may impact the audit, including how appropriate audit evidence may be obtained in a blockchain-enabled world</li> <li>Put into practice the <i>2013 Framework</i> to evaluate risks and control implications related to the use of blockchain</li> </ul>
Internal auditors, management accountants, and others concerned with internal control matters	
External auditors	<ul style="list-style-type: none"> <li>Build knowledge and expertise of blockchain</li> <li>Understand how blockchain may impact the audit, including how sufficient appropriate audit evidence may be obtained in a blockchain-enabled world and how blockchain may be used for audit purposes</li> <li>Work within the firm and with third-party audit tool developers to develop necessary tools (e.g., to understand the internal controls and audit blockchain transactions)</li> </ul>
Academics	<ul style="list-style-type: none"> <li>Leverage information and educational materials, webcasts, training sessions, and other resources to help educate students</li> <li>Consider potential research projects related to the implementation of blockchain and its use cases to help evaluate the implications of blockchain and effective internal control</li> <li>Explore new knowledge, innovative practices, and standards and regulations in this evolving space</li> </ul>

<sup>18</sup> Deloitte's 2020 Global Blockchain Survey, *From Promise to Reality*, Deloitte Insights.

<sup>19</sup> When people talk about industries being disrupted by blockchain, certain industries tend to rise to the top of the list. Defining characteristics of these industries include those with supply chains, longer term record-keeping needs, and large volumes of repetitive detail (e.g., financial services; health care, trade, and supply chain management).

Even while blockchain technology is evolving, the financial reporting stakeholder community can jointly work to better understand the challenges and risks, ways to remediate, and leading practices such that the potential benefits are realized. Stakeholders must realize that adoption is likely to move forward (even given the associated risks) regardless of whether such activities occur. If efforts are not made now, the knowledge, learning, and application gap will widen, and more effort will be required later to react to the challenges with the technology and its adoption.

The benefits of blockchain specific to financial reporting reliability will be maximized only if those who understand financial reporting, internal controls, and third-party assurance are actively involved in the evolution of the blockchain ecosystem as well as related regulation and guidance. Further, the potential benefits of blockchain to financial reporting stakeholders will be maximized only in conjunction with coupling with other technologies, such as, AI and IoT.



## APPENDIX 1. TECHNICAL APPENDIX

### Short History of Blockchain

The initial blockchain adoption was primarily for Bitcoin. As highlighted in the seminal Satoshi Nakamoto paper, “*Bitcoin: A Peer-to-Peer Electronic Cash System*” (2008),<sup>20</sup> Bitcoin was designed for peer-to-peer payments (value exchange) without the need for a central bank or intermediary; this has led to excitement by some and concern among others that digital assets could pose a legitimate threat to traditional financial services.

While digital assets and their volatility in value made headlines, market participants began to investigate the underlying technology, blockchain, and its potential as a new means of connecting parties. Given blockchain’s rapidly evolving use cases, global efforts to standardize and utilize the technology for a wide variety of purposes beyond Bitcoin have gained steam. With blockchain functionality (e.g., facilitating the transfer of digital assets in near real time), organizations have the opportunity to work differently, with new business models and value chains, and increased speed toward product or delivery.

#### When did blockchains begin?

##### The proto-blockchain

Blockchain’s beginning goes back to the early 1990s when Dr. Stuart Haber and Dr. Scott Stornetta published a number of academic research papers<sup>21</sup> related to using math and cryptography to prove document integrity by linking new batches of document metadata to an existing chain. This append-only structure leverages time-stamping and digital signatures, with the goal to ensure the integrity of data throughout the chain.

##### Bitcoin’s blockchain

Nakamoto’s paper, which does not use the term blockchain, cites and expands on Haber and Stornetta ground-breaking work to support electronic cash and peer-to-peer exchange. The goals included eliminating the need for a single financial intermediary, preventing double spending,<sup>22</sup> and incentivizing the decentralized participants to maintain the decentralized network and do the work to add the new records. “Bitcoin is **open-source**; its design is public, nobody owns or controls Bitcoin and everyone can take part.”<sup>23</sup> Bitcoin’s ability to rely on the system without needing to trust the participants is the source of the phrase “trustless.”

##### Later blockchains, adding tokens, and smart contracts

After Bitcoin, a number of other blockchains sprouted (e.g., the ethereum<sup>24</sup> blockchain). These added the ability to design custom digital assets called tokens and introduced a powerful programming environment called smart contracts.

<sup>20</sup> <https://bitcoin.org/bitcoin.pdf>.

<sup>21</sup> Such as “How to Time-Stamp a Digital Document”; [www.anf.es/pdf/Haber\\_Stornetta.pdf](http://www.anf.es/pdf/Haber_Stornetta.pdf).

<sup>22</sup> With physical coins and bills, only one person at a time can be in possession. However, when using digital assets that were not designed to deal with the “double spend problem”, the proof of availability of an open balance can be promised to multiple parties at the same time. Bitcoin sought to minimize the problems this might cause.

<sup>23</sup> <https://bitcoin.org>.

<sup>24</sup> More about Ethereum, the catalyst for its development, and how it expanded on Bitcoin’s blockchain with tokens and smart contracts, can be found at <https://ethereum.org/>.

Some of the key concepts associated with blockchain as used in this paper include the following:

Table 7. Key Concepts Associated with Blockchain	
Concept	Explanation
<b>Consensus mechanisms (or protocols)</b>	With decentralized control of a blockchain, some means of gaining agreement on 1) the way transactions are checked against a base set of rules and making sure the blockchain contains a consistent set and 2) the ordering of validated transactions within the shared, distributed information is necessary. This means of gaining agreement is known as a <i>consensus mechanism</i> . (Bitcoin accomplished agreement through incentives by compensating the participants, called “miners.”)
<b>Consortium blockchain</b>	Consortium blockchains are normally permissioned, but some are built upon public blockchains. Consortium blockchains include different organizations that have come together and agreed to jointly use a blockchain.
<b>Decentralized database</b>	Blockchain is often described as a “decentralized” database. A “database” is usually described as structured data organized to be easily accessed, managed, updated, and queried, with a focus on retrieval. This is not true of all blockchains; some are designed to be opaque and prevent any form of third-party analysis.  A major distinction between blockchain with digital assets and a database is the possibility of blockchain being the sole record keeping device for the digital assets. <sup>25</sup> Blockchain excels where a disparate group of people want to share information but not have to rely on one of the parties to act as the intermediary.
<b>Digital asset</b>	The term digital asset as used in this paper is referring broadly to digital records, made using cryptography for verification and security purposes, on a distributed ledger (e.g., blockchain). Digital assets, as defined by the AICPA, <sup>26</sup> may be characterized by their ability to be used for a variety of purposes, including as a medium of exchange, as a representation to provide or access goods or services, or as a financing vehicle, such as a security, among other uses. The rights and obligations associated with digital assets vary significantly, as do the terms used to describe them.
<b>Forks</b>	<p>Forks are an important tool that have been used widely in public blockchains like Bitcoin and Ethereum. As the name would imply, when a blockchain forks, some decision is made that results in two potentially different paths. Two separate chains will now have commonality up to the point of the fork, after which different sets of rules, different additions to data, and sometimes completely different assets will apply. Groups may choose to fork a blockchain in order to make a correction to the “immutable” blockchain on which they are based.</p> <p>In the fork illustrated in the following example, holders of the original digital asset also became holders of another digital asset in the new chain created by forking the original chain. Sometimes, Bitcoin and Ethereum have forked solely in order to apply new rules.</p>
<b>Hash</b>	A hash is a cryptographic, one-way algorithm for taking data of any size and converting it to a unique piece of information of a fixed size. With blockchain, each block on a blockchain is linked to the prior block with such a unique identifier.
<b>Immutability and record integrity</b>	Immutability refers to the append-only nature of a blockchain. The design of blockchain as append-only with cryptography means that information, once written to the blockchain, is very difficult to alter. Although corrections are still possible, corrections will need to be reflected as adjustments rather than directly as corrections to an existing transaction. Blockchain promises record integrity, but it does not promise that the records themselves reflect lawful or appropriately classified transactions.
<b>Miners</b>	Bitcoin accomplished a consensus through incentives, by compensating the participants (called miners) who exert effort and provide computational power to solve a computationally difficult mathematical puzzle – one that is difficult to perform but easy to check – a method known as “proof-of-work.” The Bitcoin design was purposefully challenging. Other methods, including giving more credibility to those who hold more of the digital asset themselves, called proof-of-stake, are also being used. As the original Bitcoin white paper notes, “What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.” <sup>27</sup>

<sup>25</sup> For example, the Bitcoin ecosystem focuses on tracking Bitcoin, a digital asset with value that stands on its own (or not). The Ethereum platform has its primary digital asset, Ether, but also permits the creation of customized (bespoke) mutually exchangeable tokens (ERC\* 20) and other non-fungible tokens (ERC 721); many digital assets are created using Ethereum.

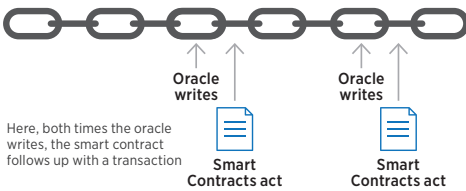
<sup>26</sup> AICPA, “Practice Aid: Accounting for and Auditing Digital Assets,” December 2019.

<sup>27</sup> <https://bitcoin.org/bitcoin.pdf>.

**Table 7. Key Concepts Associated with Blockchain (cont.)**

Concept	Explanation
<b>Nodes</b>	Each computer on a blockchain network is known as a node.
<b>On-chain transactions, off-chain transactions</b>	On-chain transactions are the transactions available on the distributed ledger and are also potentially visible to all the members of the blockchain network. Off-chain transactions represent the movement of assets or recording of related information outside of the blockchain.
<b>Open-source</b>	An open-source model is a collaborative development and distribution model. It encourages those with common development interests to work together to produce something cost-effectively and with a greater eye to quality through numbers than individual commercial developers could create on their own.
<b>Oracle</b>	Oracles are a means of writing information to a blockchain as a record so smart contracts can monitor the records for changes and then act on them. Because oracles provide important input used to execute the terms of smart contracts, implementing controls over such oracles is important. It is important to check that an entity obtains periodic evidence about safeguards used to secure third-party oracles, if such are used. In addition, where IoT devices are used to act on external activities as part of the oracle, additional risks and controls should be considered.
<b>Private (permissioned)</b>	Private blockchains require permission from the owner or the protocols set up by the developer to read, write, or otherwise access the blockchain. It is possible, but unusual, for a private blockchain to be permissionless.
<b>Public (typically permissionless)</b>	Permissionless blockchains do not require permission to read or otherwise access the blockchain. They do have specific rules on who can write, also known as consensus. It is possible for a public blockchain to be permissioned.
<b>Private and Public Keys</b>	<p>Blockchains use public and private keys (see following figure) for the authorization of the movement of digital assets from one blockchain address to another. Although common in security and especially encryption,<sup>28</sup> the use of such keys has not been part of daily business activities. Digital asset transfers are authorized using the private key, and managing these keys is a new and critical responsibility in blockchain environments. Much like multiple written signatures being required for banking transactions, multiple keys may be required for digital asset transactions (multisignature or multisig). And much like people counterfeiting someone else’s signature, someone with access to someone else’s keys can act without the key owner’s permission.</p> <p>As seen in the following figure, a large random number is used to <i>seed</i> standardized mathematical algorithms to create a private key (kept secret, but used to authorize the movement of digital assets from a specific blockchain address). Further algorithms create the public key and, from the public key, the blockchain address, the tracking number for digital asset balances. It is very easy to determine the address from the seed and the key. It is, however, practically impossible to go the other way – from address to public key, public key to private key, or private key to seed.</p> <p><b>Cryptographic Seed</b> → <b>Math happens here!</b> → <b>Private Key</b> → <b>Public Key</b> → <b>Public Blockchain Address</b></p> <p>Random information used to create key pairs</p> <p>9183801836519301 693737131890007 124663901033018</p> <p>A number derived from this: kept secret</p> <p>A number derived from the private key</p> <p>A number derived from the public key (Bitcoin, Ethereum, etc.)</p>
<b>Rollback</b>	<p>A chain rollback is similar to copying over an existing database with an older version of that database due to data corruption or other problems. When a situation arises where there is sufficient support to “undo” later transactions, the chain is restored to a prior state, and a process of rewriting the necessary transactions after that point is conducted.</p> <p>In the following figure, a series of transactions after block 125,998 are invalidated/removed, resulting in a rollback. With public blockchains like Bitcoin, this is not a simple process and has severe repercussions given blockchain’s reputation as immutable. Where there is more centralized control, this could be easier to accomplish, although such an action would be obvious to observers.</p> <p><b>Original Chain</b> 1 2 ... 125,998</p> <p>A problem occurs with a transaction in block 125,998, but isn't caught until much later</p> <p>The original chain is recreated from the point at which the problem occurred (which is the point at which the chain is rolled back to)</p>

<sup>28</sup> Encryption is a two-way process where information is altered in a way that only those with appropriate knowledge or tools can re-create the original message. It is used to deny intelligible content to an unauthorized interceptor.

Table 7. Key Concepts Associated with Blockchain (cont.)	
Concept	Explanation
Smart Contracts	<p>Smart contracts in blockchain are computer programs stored on a blockchain that “self-execute” and where the outcome of any execution of the program is recorded on that blockchain. Although not limited or designed specifically to act like a legal contract, these programs can drive the recording of a transaction or the exchange of a digital asset automatically given the necessary input. When conditions are met, either from transactions occurring naturally on the blockchain or by transactions written by external sources, called oracles, the smart contract will create transactions autonomously.</p> 
Tokens	<p>Tokens are a type of digital asset, which can be new digital assets on their own, represent intangible assets (such as voting rights), or work as a digital proxy to physical assets.</p>
Wallet	<p>Wallets are used to manage keys. A cold wallet is not connected to the Internet. A hot wallet is connected to the Internet.</p>

## APPENDIX 2. KEY INSIGHTS: 10 THINGS TO KNOW ABOUT BLOCKCHAIN

The 10 things organizations should know about blockchain include the following:

- 1 Information about blockchain in the news and on the Internet is often misleading or incorrect.**  
 In gaining an understanding of blockchain refer to reliable sources. Be aware there is not one blockchain (i.e., “the Blockchain”) and use of a blockchain will not instantly and magically link every organization together in commerce in a fully trustworthy, self-auditing environment, where the encrypted data within will open to only the right people at the right time. In fact, there are many blockchains, most of which do not easily speak to each other, many things that can go wrong, and much of the information needed is not on the blockchain itself.
- 2 Blockchain encompasses far more than digital assets; the benefits it can bring to an organization can be substantial.**  
 Blockchain technology goes beyond digital assets and use cases are broad across industries. Blockchain became best known for Bitcoin, but the use cases are much wider now (e.g., supply chains, finance, insurance, and other areas). As the global economy moves toward digital assets, blockchain technology may affect everything from the products and services organizations provide and how they provide them, to the way entities

manage internal record-keeping and data management systems and handle the processing of transactions.

- 3 Blockchain is not magic; it comes at a cost and doesn’t eliminate all risks. In fact, it introduces new risks.**  
 Blockchain does not address all risks by replacing all functions of an ERP system nor does it ensure compliance with all rules and requirements. In fact, with blockchain come new risks to consider for new asset classes and processes. When participating in a blockchain, each participant should understand the responsibilities, operating and governance models, transaction rules, security protocols, incentives, penalties, and processes for joining and leaving the consortium, if applicable.
- 4 Knowing how blockchain technology works is crucial for evaluating, preparing for, and managing blockchain’s impact on internal control and the organization as a whole.**  
 Blockchain will create significant benefits for the right use cases, such as increasing efficiency and reducing human error. Generally, blockchain is most worth considering when:

  - There are multiple parties and intermediaries to a process, all recording the same information

- There is a reconciliation-heavy process for managing the business and its relationships
- There is substantial manual data entry and tracking
- Stakeholders require different aggregations of reports and frequent ad hoc reporting

**5 Blockchain has both technology and governance implications.**

New blockchain controls will inherently have a heavy technology focus. It is also important, however, to consider issues such as governance, document and data retention, privacy laws, competitive advantage, reputation, accountability, and information visibility.

**6 Blockchain will not make management, accountants, or auditors less relevant, although it will impact what they do and how they do it.**

Blockchain is not currently capable of judgments, interpretation, valuations, accrual accounting, tracking commitments and contingencies, or providing assurance. Further, blockchain will change how financial transactions are recorded and analyzed, how reconciliations are performed, and how auditors obtain evidence. The use of blockchain may increase the demand for service auditor reports on the controls around the technology (See sidebar on page 5). Understanding and monitoring the evolving accounting and financial reporting rules is important.

**7 Blockchain requires new skill sets (e.g., data science for greater hindsight, insight, and foresight) and new collaboration within and across organizations.**

Blockchain will create a demand for different skill sets with expertise in the technology (and its ramifications)

to develop, implement, and monitor the blockchain. Blockchain education and upskilling will be critical. New collaborative skills and blending of management, technical, and legal skills – both within and across organizations – will be necessary.

**8 Now is the time to educate and engage stakeholders throughout the organization.**

Early engagement throughout the organization will be important to consider the potential blockchain use cases, skill sets and training needed, performance requirements, scalability, integration with present systems, implications on evidence used to support the books and records, and resource needs. Creating both a short-term and long-term plan may be needed.

**9 Blockchain is still in flux and continues to evolve.**

Some analysts say any solution implemented today will have to be redone in a few years.<sup>29</sup> However, once the industry or regulatory environment clarifies the needed functionalities of blockchains, digital assets, and programming languages, there will be increased stability.

Academics, collaborating with practitioners, could be indispensable in advancing thought leadership, as well as helping cope with real world practical challenges and proposing solutions.

**10 Adoption of blockchain may not be a choice.**

Blockchain will likely have an impact on all organizations through direct investments in digital assets, indirect investments in digital assets, creation of their own permissioned blockchain, participation in an external permissioned blockchain, or other activities. There may be a pull for implementation from customers, suppliers, partners, and the government.

<sup>29</sup> Gartner has suggested that 90% of 2019's blockchain implementations will require replacement by 2021. [www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain](http://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain).





## APPENDIX 3. BLOCKCHAIN, FINANCIAL REPORTING ASSERTIONS, AND AUDIT EVIDENCE

Management implicitly or explicitly makes assertions regarding the recognition, measurement, and presentation of information in the financial statements and related disclosures. The work of the auditor is to obtain sufficient appropriate audit evidence to support their opinion. Audit evidence comprises both information that supports and corroborates management's assertions, and information that potentially contradicts such assertions.

The following table highlights ways in which blockchain may present challenges with respect to how companies provide sufficient and appropriate audit evidence to support management's assertions surrounding assets or transactions stored on a blockchain.<sup>30</sup>

**Table 8. Management's Assertions and Blockchain**

Concept	Explanation
<b>Valuation</b>	Most use of blockchain is to track a quantity of something (such as a digital asset balance), but the value of the item being tracked is not necessarily maintained in the blockchain. In addition, the determination of the value of digital assets may prove difficult in the event that there is little or no observable market data to support the value of these assets or large variations in market data (e.g., Level 3 assets, most illiquid and hardest to value, per ASC Topic 820 <sup>31</sup> ).
<b>Existence</b>	Often, the existence of digital assets is solely dependent on the evidence that can be obtained from a blockchain. Although blockchain has been developed to reduce tampering within transaction processing and recording, this does not, by itself, render the information stored on the distributed ledger fully reliable. The reliability of the information obtained from the blockchain is heavily dependent on the effectiveness of the underlying technology and relevant controls implemented to support the system. Therefore, solely providing information from a blockchain may not be deemed sufficient appropriate evidence to validate the existence of an asset. In many cases, additional procedures are warranted (e.g., test of internal controls related to the blockchain and security of the private keys to the digital assets).
<b>Allocation</b>	Blockchain information – such as blockchain-based tracking of shares, voting rights, or other relationships – can be used to support allocation calculations. However, additional procedures may be needed to support the reliability of information obtained from the blockchain to support such allocation calculations.
<b>Occurrence</b>	As with existence, information obtained from the blockchain may not, by itself, support the occurrence assertion. Additional procedures may be necessary to prove the reliability of information stored on the blockchain and hence the occurrence of a transaction. Furthermore, the pseudo-anonymous nature of transactions on the blockchain could provide users with the opportunity to engage in fictitious transactions or transactions with related parties that have no economic substance, thereby inflating revenues.
<b>Completeness</b>	Where a blockchain is the only record of transactions, it can serve as a complete record; however, the completeness of transactions stored on the blockchain will be dependent on the reliability of the blockchain technology as well as the controls implemented by the entity to ensure its books and records are appropriately capturing all transactions. Further, where information is recorded in whole or part in another system, blockchain does not support completeness. Controls would have to be in place to ensure that all activity, on-chain or off, and all detail, on-chain or off, is available and completely recorded.
<b>Classification</b>	The classification of a digital asset may prove difficult, because accounting guidance and precedent surrounding this topic is still evolving. Furthermore, companies will need to objectively evaluate the purpose and use of the asset in order to determine the appropriate classification of such assets.
<b>Understandability</b>	Blockchain does not take into account the need for any reporting or summarization of the information in an understandable fashion and does not have a function to do so. Management will need to determine what data from the blockchain will be useful to support the development of its financial statements and an appropriate method for obtaining and summarizing such data. Similar to the classification assertion, accounting guidance and precedent surrounding this topic is still evolving and due care should be taken in determining the presentation of digital assets within an entity's financial statements.
<b>Accuracy</b>	Serving as the record for digital assets, blockchain stores the history of all transactions and balances. It does not mean that information within the blockchain is accurate, only that records keep their integrity.
<b>Presentation</b>	See considerations surrounding understandability.

<sup>30</sup> Eric Cohen, "Will Blockchain Make Auditors Obsolete?", ThinkTWENTY20, Spring 2019. [www.thinktrenty20.com/images/docs/Spring-Issue-2019.pdf](http://www.thinktrenty20.com/images/docs/Spring-Issue-2019.pdf), accessed June 16, 2020.

<sup>31</sup> Fair Value Measurement (Topic 820), <https://asc.fasb.org/imageRoot/81/118196181.pdf>.

Table 8. Management's Assertions and Blockchain (cont.)

Concept	Explanation
<b>Cutoff</b>	As a complete record of all related transactions, where records or blocks are time-stamped as they are written to the blockchain, there are capabilities to assess cutoff of recording dates. However, there is no inherent capability for accounting recognition dating, or concepts of accruals, prepaids, or matching expenses with revenues.
<b>Obligations and Rights</b>	Generally, there are no written title agreements associated with digital assets to support the rights and obligations assertions. Although procedures such as signed messaging may be used to demonstrate control over a private key (and hence rights to an asset) operational limitations may not allow for these procedures to be completed. Furthermore, these procedures may depend on the reliability of the underlying blockchain technology, thereby warranting the performance of additional procedures (e.g., test of internal controls). Finally, although signed messaging procedures may demonstrate control over the private key, there is still the risk that the private key may not be solely controlled by the organization (i.e. other parties may have access to the private key and hence control or ownership of the associated assets).



## SUPPLEMENTARY RESOURCES AND REFERENCES, INCLUDING THOSE PROVIDED BY COSO BODIES

This paper has been written to complement the many helpful documents and other resources provided by the sponsoring organizations and other related stakeholders. Examples of those documents relevant to this discussion include:

### AAA

<https://aaahq.org/Meetings/2018/BlockchainAAA>

### AICPA

[www.aicpa.org/interestareas/informationtechnology/resources/blockchain.html](http://www.aicpa.org/interestareas/informationtechnology/resources/blockchain.html)

### FEI

[www.financialexecutives.org/Research/News/2017/Blockchain-and-the-Future-of-Financial-Reporti-\(1\).aspx](http://www.financialexecutives.org/Research/News/2017/Blockchain-and-the-Future-of-Financial-Reporti-(1).aspx)

### IMA

Frans Roozen, Ph.D.; Bert Steens, Ph.D.; and Louis Spoor, "Technology: Transforming the Finance Function and the Competencies Management Accountants Need," *Management Accounting Quarterly*, Fall 2019, [www.imanet.org/insights-and-trends/management-accounting-quarterly/maq-index/2019/fall-2019?ssopc=1](http://www.imanet.org/insights-and-trends/management-accounting-quarterly/maq-index/2019/fall-2019?ssopc=1)

Reina G. Wiatt, CMA, CPA, "From the Mainframe To the Blockchain," *Strategic Finance*, January 2019, <https://sfmagazine.com/post-entry/january-2019-from-the-mainframe-to-the-blockchain/>

Natalia Maslova, CMA, CTP, PMP, "Blockchain: Disruption and Opportunity," *Strategic Finance*, July 2018, <https://sfmagazine.com/post-entry/july-2018-blockchain-disruption-and-opportunity/>

### IIA

[www.theiia.org/centers/aec/Pages/blockchain-risks-opportunities.aspx](http://www.theiia.org/centers/aec/Pages/blockchain-risks-opportunities.aspx)

### Other relevant sources

#### ACCA Global: Divided We Fall, Distributed We Stand

[www.accaglobal.com/uk/en/technical-activities/technical-resources-search/2017/april/divided-we-fall-distributed-we-stand.html](http://www.accaglobal.com/uk/en/technical-activities/technical-resources-search/2017/april/divided-we-fall-distributed-we-stand.html)

#### ICAEW: Blockchain and the Future of Accountancy

[www.icaew.com/-/media/corporate/files/technical/information-technology/technology/blockchain-and-the-future-of-accountancy.ashx](http://www.icaew.com/-/media/corporate/files/technical/information-technology/technology/blockchain-and-the-future-of-accountancy.ashx)



## ABOUT THE AUTHORS



### Jennifer Burns, Partner, Deloitte & Touche LLP

Jennifer is a Partner in the National Office of Deloitte & Touche LLP and has over twenty-five years of experience in regulatory, standard-setting, and quality matters impacting the performance of audits. She currently leads Deloitte's National Office efforts related to emerging areas of assurance services (including in the areas of artificial intelligence, blockchain, sustainability and other third-party assessments) and consults with engagement teams regarding the appropriate application of professional standards. She also engages regularly with audit committees and clients regarding regulatory developments impacting the profession.

Jennifer is a member of the AICPA's Assurance Services Executive Committee, driving its mission to help the profession meet evolving market needs. She interacts with other standard-setting and regulatory entities including the PCAOB, SEC, IAASB, and COSO, representing the views of the firm. Jennifer also served on the task forces advising COSO in its development of its *Internal Control over Financial Reporting Small Business Guidance* (2006), *Guidance on Monitoring Internal Control Systems* (2009), and *COSO's Internal Control- Integrated Framework* (2013).

Previously, Jennifer was a Professional Accounting Fellow at the U.S. Securities and Exchange Commission in the Office of the Chief Accountant, where she was involved in the oversight of the development of professional standards and the implementation of requirements related to the Sarbanes-Oxley Act.

Jennifer is a CPA, licensed in Washington, D.C., California, and Nevada, a member of the AICPA, and graduated cum laude from Claremont McKenna College in Claremont, California.



### Amy Steele, Partner, Deloitte & Touche LLP

Amy is a Partner in the National Office of Deloitte & Touche LLP and leads audits of public and private companies in the Technology and Media industries. Amy has deep experience in regulatory, standard-setting, and audit quality, and leads strategies to enhance quality, and innovate and transform audits across Deloitte's global organization. Amy is Deloitte's U.S. and Global audit methodology leader for blockchain and digital assets. Amy is also the lead partner for Deloitte's emerging assurance services – focused on the expanded role of the audit professional and the impact of technology in audits. Additionally, Amy leads Deloitte's audit methodology for revenue and consults with engagement teams on complex applications of auditing standards. In these roles, Amy engages often with regulatory agencies and profession-wide bodies.

Amy chairs the AICPA Digital Assets Working Group, leading the profession in developing auditing and accounting guidance for digital assets. Amy also serves on the Center for Audit Quality Emerging Technologies Task Force and Cybersecurity Task Force. Amy is an active thought leader in the business community, is sought out for her views on issues impacting financial reporting and the audit profession and communicates to broad audiences and regulators on technical topics.

Previously, Amy served as Associate Chief Accountant in the Office of the Chief Accountant of the SEC where she had a unique opportunity to support the Office of the Chief Accountant in its role as the principal advisor to the Commissioners on profession-wide auditing matters and oversight of the PCAOB. Additionally, in this role, Amy consulted on technical audit and internal control matters with auditors and various SEC offices and divisions and was the SEC's official observer to COSO during the development of COSO's *Internal Control - Integrated Framework* (2013).

Amy graduated Magna Cum Laude, University of Washington and with honors from the Master of Professional Accounting, University of Washington. She is a member of the AICPA and holds her CPA license in Washington and Connecticut.



### Eric E. Cohen

Eric Cohen is the proprietor of Cohen Computer Consulting, a consultancy focused on emerging accounting and audit technologies, including audit data standards, blockchain, continuous audit, sustainability/corporate responsibility, and XBRL. He is a co-founder of the Extensible Business Reporting Language (XBRL) movement and “inventor” of XBRL’s Global Ledger Taxonomy Framework (XBRL GL). As an ambassador of XBRL, he has worked in cooperation with virtually every other standards effort attempting to standardize accounting and audit data, and a long cooperation with UN/CEFACT led to his assuming the role of UN/CEFACT Domain Coordinator for the Accounting and Audit Domain.

Mr. Cohen is a prolific author and willing speaker, teacher and trainer, having written or contributed to numerous books (including *Guide to Customizing Accounting Software* (CTS) and *Accountant’s Guide to the Internet* (John Wiley), as well as hundreds of articles for the business, professional and academic press. He enjoys a long partnership with the academic community, cooperating with many professors in research and curriculum building on XBRL, continuous audit, and related areas of interest.

It was this collaboration that led to his work in blockchain and distributed ledger technologies; he serves as a national expert to ISO/TC 307 Blockchain and Distributed Ledger Technologies, where he focuses on standards development around governance, interoperability, and audit guidance. Mr. Cohen is a member of the NYSSCPA Digital Assets Committee and was the Chair of the 2019 NYSSCPA/FAE Digital Assets Conference.



### Dr. Sridhar Ramamoorti

Dr. Sridhar Ramamoorti, ACA, CPA/CITP/CFF/CGMA, CIA, CFE, CFSA, CGAP, CGFM, CRMA, CRP, MAFF, is an Associate Professor of Accounting at the University of Dayton, Ohio. To remain engaged with practice issues, he is affiliated as a principal with two consulting firms, Quetzal GRC LLC that offers risk advisory services, and the Behavioral Forensics Group LLC that provides fraud risk mitigation, detection, and investigation services. Previously, he was an Associate Professor of Accounting and a Director of the Corporate Governance Center, Michael J. Coles College of Business, Kennesaw State University in Kennesaw, Georgia.

Dr. Ramamoorti has a unique, blended academic-practitioner background with over 35 years of experience in academia, auditing, and consulting. After finishing his Ph.D. from The Ohio State University, he initially served on the accountancy faculty of the University of Illinois. Subsequently, he progressed successively as a principal with Andersen’s Professional Standards Group, National SOX Advisor for EY, and corporate governance partner with Grant Thornton, all in Chicago, Illinois. He briefly led the governance, risk, and compliance (GRC) professional services practice of Infogix, Inc. in Naperville, Illinois, prior to re-entering academia.

Dr. Ramamoorti was a member of the authoring/development teams of the 2009 *COSO Guidance on Monitoring Internal Control Systems*, 2010 ISACA guidance on *Monitoring Internal Control Systems and IT*, *The Audit Committee Handbook* (5<sup>th</sup> ed., Wiley, 2010), *Internal Auditing: Assurance and Advisory Services* (IIA, 2017, 4<sup>th</sup> ed), and *A.B.C.’s of Behavioral Forensics* (Wiley, 2013) on the psychology of fraud that has been presented to the FBI Academy and at several Conferences. He has published over 60 papers and articles in academic and professional journals and serves on numerous editorial boards.

Active in the profession, he is a member of all five sponsoring organizations of COSO and has served as a Trustee for the IIA and FEI Research Foundations. He is a former member of the Standing Advisory Group of the Public Company Accounting Oversight Board (PCAOB). Over the past two decades, Dr. Ramamoorti has been a speaker in 16 countries.

## ABOUT COSO

---

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM), internal control, and fraud deterrence. COSO's supporting organizations are the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and the Institute of Internal Auditors (IIA).



The Association of  
Accountants and  
Financial Professionals  
in Business



## ABOUT DELOITTE

---

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients.

Please see [deloitte.com/about](https://deloitte.com/about) for a detailed description of DTTL and its member firms. Please see [deloitte.com/us/about](https://deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting..

## Deloitte.

.....

This publication contains general information only and none of COSO, any of its constituent organizations or any of the authors of this publication is, by means of this publication, rendering accounting, business, financial, investment, legal, tax or other professional advice or services. Information contained herein is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Views, opinions or interpretations expressed herein may differ from those of relevant regulators, self-regulatory organizations or other authorities and may reflect laws, regulations or practices that are subject to change over time. Evaluation of the information contained herein is the sole responsibility of the user. Before making any decision or taking any action that may affect your business with respect to the matters described herein, you should consult with relevant qualified professional advisors. COSO, its constituent organizations and the authors expressly disclaim any liability for any error, omission or inaccuracy contained herein or any loss sustained by any person who relies on this publication.

Governance and Internal Control



**COSO**

Committee of Sponsoring Organizations  
of the Treadway Commission

[coso.org](http://coso.org)

Governance and Internal Control



BLOCKCHAIN  
AND  
INTERNAL CONTROL:  
THE COSO PERSPECTIVE

***COSO***

Committee of Sponsoring Organizations of the Treadway Commission

[coso.org](http://coso.org)

