Journal of Corporate Governance, Insurance, and Risk Management
https://www.acadlore.com/journals/JCGIRM

Assessing the Impact of Blockchain Technology on Internal Controls Within the COSO Framework

Gülçin Kazan[1*], Tuğçe Uzun Kocamış[2]

[1] International Trade and Finance, Istanbul Sabahattin Zaim University, 34303 Istanbul, Turkey
[2] Accounting and Tax, Istanbul University-Cerrahpaşa, 34320 Istanbul, Turkey

[*] Correspondence: Gülçin Kazan (gulcin.kazan@izu.edu.tr)

Received: 05-03-2023 **Revised:** 06-10-2023 **Accepted:** 06-16-2023

Citation: Kazan, G. & Kocamış, T. U. (2023). Assessing the impact of blockchain technology on internal controls within the COSO framework. *J. Corp. Gov. Insur. Risk Manag.*, *10*(1), 86-95. https://doi.org/10.56578/jcgirm100110.

Abstract: Developments in Blockchain technology and their increasing adoption have prompted examination of intersections with organizational internal control systems. Technological solutions leveraging blockchain reportedly enhance operational effectiveness and efficiency, core internal control objectives. Such improvements could increase financial and non-financial reporting reliability and facilitate regulatory compliance. The Committee of Sponsoring Organizations' (COSO) internal control framework provides a systematic methodology for designing and implementing effective controls utilizing blockchain technologies. Within the COSO 2013 framework's context, this study aims to identify risks that may arise from blockchain technology integration into financial reporting processes and outline corresponding control formulations. Specific focal points involve risk evaluation associated with blockchain technology adoption and control implementation proposals addressing identified issues. If properly designed, controls may optimize blockchain technology capabilities for transparent, accountable, and sustainable value generation. This initial examination offers strategic guidance on evidence-based advancement of business-community symbiosis locally and globally through continuous policy evolution. Regional contextualization and adaptability to emerging complexities will determine durability of theoretical edifices established.

Keywords: Blockchain; Blockchain technology; COSO 2013; COSO framework; Internal control; COSO components

1. Introduction

Blockchain technology has experienced accelerated development and adoption since their emergence in 2009. Originally applied to digital currency transactions, these solutions now influence diverse industries including banking, finance, and utilities. Their transformative potential for global digital business environments has prompted examination of intersections with organizational functions.

Blockchain integration into financial reporting and internal control structures necessitates evaluation on an application-specific, firm-level basis, encompassing risk analyses and best course determination. Conceptually analyzed, Blockchain technology may enhance reporting reliability and regulatory compliance through improved operational effectiveness and efficiency—primary internal control objectives. However, new risks and challenges warrant consideration.

The Committee of Sponsoring Organizations' (COSO) internal control framework supplies a systematic methodology for designing, implementing, and assessing effective controls amid technological change. Within this study's COSO 2013 framework context, potential blockchain technology adoption risks associated with financial reporting are identified. Corresponding control implementations addressing issues are proposed.

By systematically examining blockchain technology's impact on the control environment, risk assessment, control activities, information/communication, and monitoring components, this research aims to contribute understanding at the intersection of emerging technologies and established norms. Following sections explore key blockchain and COSO concepts. Potential effects on individual framework elements are then discussed through

comprehensive analysis, differentiating compatibility scenarios.

Valuable insights are provided for organizations, practitioners, and scholars navigating continuously evolving internal control paradigms. While conceptually Blockchain technology may optimize value generation sustainably and transparently, proper contextualization and adaptability remain imperative. Regional particularities and emerging complexities will determine theoretical durability over the long term.

2. Block Chain Technology and COSO Framework

2.1 Blockchain: An Overview

Blockchain can be characterized as a form of digital ledger or registry, where data is chronologically stored in interconnected blocks, each encrypted for secure storage (Nofer et al., 2017). Each block encapsulates information indicating the time of its recording, alongside the data intended for registration. Data persistence occurs in a manner that allows public accessibility and verification, thereby enabling anyone to possess a copy of the registry. This decentralization ensures the transparency and security of blockchain records, independent of a single governing center.

The immutable nature of the blockchain confers permanency to the network, contrasting starkly with traditional centralized systems. This immutability persists even in the face of disruptions to individual nodes, instilling trust in the network's structure. Consequently, the necessity to evaluate the trustworthiness of agents or other network participants is eliminated; trust in the system suffices (Nofer et al., 2017).

In the information age, the speed and accuracy of information are paramount for businesses. The blockchain network facilitates swift and secure tracking of various processes including orders, payments, production, and supply. Access to this instantaneous and transparent information is restricted to authorized network members. Stored in an unalterable ledger, this information is imbued with a permanent, indelible, and unalterable transaction history, redefining the audit process as a swift, efficient, and cost-effective procedure (Liu et al., 2019).

The implementation of blockchain introduces new roles for auditors, such as reviewing specific transactions, confirming the existence of digital assets, and verifying consistency between information in a blockchain and the physical world (Liu et al., 2019). The end-to-end visibility of transaction details fosters trust among network members and engenders efficiency and novel opportunities (Lim, 2023). Modern blockchain applications must address multiple requirements, including security, privacy, throughput, size and bandwidth, performance, availability, data integrity, and scalability (Koteska et al., 2017).

Key characteristics of the blockchain can be summarized as follows (Lim, 2023):

- Distributed: Blockchain's fundamental feature is the distributed recording, storage, and updating of data, as opposed to centralization.
- Transparent: The blockchain system affords transparency in data recording to all nodes, and retrospective data verification, enhancing its reliability.
- Autonomous: The consensus structure enables secure data transfer across all nodes in the blockchain system, obviating the need for a central system.
- Immutable: Once added to the blockchain, records cannot be updated or deleted and are stored permanently. Except for various attack types, record alteration is implausible.
- Privacy of Identity: The blockchain system enables nodes to transfer data anonymously, requiring only the recipient's blockchain address.

2.2 Blockchain Technology: Effects in the Context of COSO and Internal Control

Internal controls are processes and procedures that help ensure the accuracy of information reported and communicated by the organization and the protection of business assets (Smith, 2020). COSO published its "Internal Control-Integrated Framework" in 1992. COSO means the Sponsoring Organizations Committee of the Treadway Commission. It is a private sector initiative that provides guidance and thought leadership on enterprise risk management, internal control, and fraud prevention. COSO's primary goal is to help organizations improve their governance, risk management and control processes. By following the COSO Internal Control Framework, organizations can improve their ability to manage risks, prevent and detect fraud, provide reliable financial reporting, and achieve their strategic objectives.

Since its publication, it has become the generally accepted global framework for designing, implementing, and evaluating internal controls. The COSO Framework is a system for integrating internal controls into business processes. The purpose of all these controls is to provide reasonable assurance that ethical compliance, transparency, and work in accordance with industry standards. In the COSO internal control model, which was published for the first time in 1992, regulations were made under the influence of developing technology and environmental factors, and the 2013 COSO internal control model was published. Environmental factors were especially effective in the change of COSO. However, regulations, complex laws, rules, and standards have a

significant impact on adjusting the COSO internal control model with changing expectations for fraud detection and prevention. The similarities and differences between the COSO model published in 2013 and the COSO model published in 1992 are given in the Table 1 below:

Table 1. Comparison of COSO 1992 and 2013

Similarities	Differences
1. Basic definition of internal control. 2. Cube: three goals an organization is trying to achieve; the five components of internal control necessary to achieve the objectives; It is in the form of four organizational levels at which components work. 3. Judgment is emphasized in evaluating the effectiveness of internal controls.	1. In the new framework, 17 basic principles related to the five main components have been put forward more clearly and clearly. 2. The importance of setting targets, especially in the internal control process, was emphasized. Specific objectives have been defined as a prerequisite for internal controls. 3. The new framework emphasizes the increasing importance of technology. 4. There is a broad discussion of the concept of governance. 5. A broader reporting objective is defined. Four types of reporting are mentioned. 6. Attention was paid to the fight against fraud. 7. In reporting, more emphasis is placed on non-financial types of reports.

Source: (Tadesse et al., 2022)

COSO (2013) Internal control is a broad structure influenced by an entity's board of directors, senior management, and other employees that provides reasonable assurance that the entity's core objectives are being met. The framework consists of five components: (1) the control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring activities. According to the framework, each of the five components and related principles must exist, work together, and function to minimize the risk of an organization failing to achieve its goals (COSO, 2013).

In the digital age, concepts, and principles of internal control, like COSO's Integrated Internal Control Framework, can still be applied. Technology can expand the effectiveness, efficiency, and pervasiveness of internal controls. Many organizations are already using and researching emerging technologies for their internal control processes, such as artificial intelligence for anomaly detection. It is also expected that these technologies will be used more extensively for control purposes in the future (PricewaterhouseCoopers, 2019).

When examining blockchain technology about the internal control environment, it is evident that controls will differ in a blockchain-enabled world. Hence, it is crucial to acknowledge and utilize these variances, while considering the capabilities, attributes, risks, and benefits of blockchain. Leveraging the unique characteristics of blockchain to enhance internal control will prove effective in attaining the fundamental three main objectives of internal control (Dickins & Fay, 2017).

Companies develop internal control systems to protect assets, prevent fraud, ensure the accuracy of financial records, evaluate organizational performance, and guarantee uninterrupted and efficient workflow. Conventional industries and operations are being altered by present-day digital advances, introducing novel applications to the corporate world under the umbrella of customary command processes, overall guidance milieu, hazard management, and auditing. Certain organizations are leveraging smart sensors to survey the performance of their production systems and activities, while others are implementing technologies to monitor their supply chains from raw material sourcing to finished product production. While Robotic Process Automation (RPA) is widely used in finance and operation to automatize controls and increase precision, Artificial Intelligence (AI) allows organizations to continuously monitor, visualize and recommend actions in real-time, enabling improvements in business processes and control environments. However, the use of new technologies brings risks, especially cyber security, and data privacy.

Information entering the blockchain individual information block cannot be changed after verification and validation by other network members. If organizations choose to implement this technology, they will need employees with sufficient technological infrastructure and technical knowledge (Smith & Castonguay, 2020).

In many ways, the control aspects associated with the implementation and operation of blockchain solutions are very similar to a new ERP or management system. Given financial reporting controls, financial controls and processes are likely to change fundamentally. Reconciliations, approval processes, vendor and supplier management, inclusion of digital assets in the accounting process, internal and external audit studies, continuous real-time financial reporting, and continuous monitoring are the main areas which blockchain technology can change. At the same time, it should be considered that new controls may create new risks (Burns et al., 2020).

In Table 2, the effects of blockchain applications and new technology applications on COSO internal control

system components are summarized (Deloitte, 2020).

Table 2. Implications of blockchain on five components

Components	Implications of Blockchain
Control Environment	Blockchain supports an effective control environment. However, the COSO control environment component is essentially about human behavior such as integrity and ethical values. The greater challenge is how to manage the control environment as the number of organizations or individuals involved in the chain increases.
Risk Assessment	Blockchain helps mitigate existing risks by promoting accountability, ensuring record integrity, and providing an irrefutable recording environment. It also creates new risks.
Control Activities	Blockchain and smart contracts support the effective and efficient conduct of global trade by minimizing human errors and opportunities for fraud. However, it can introduce additional complexities where many members are involved in the system and there is no single responsible party.
Information and Communication	Blockchain supports transparency, facilitates access to data and enables effective and fast communication between stakeholders. At this point, the existence and auditability of information on the chain are issues that the management should pay attention to.
Monitoring	Blockchain supports monitoring, often with more data and more granularity. It can differentiate the monitoring practices of smart contracts and standardized business rules.

Academic studies on the effect of blockchain technologies on audit and internal control systems stand out in the literature. Bonsón & Bednárová (2019), Schmitz & Leoni (2019) evaluated accounting, auditing and blockchain technologies in general. Vincent & Barkhi (2021) evaluated smart contracts applications and the effects of being included in the blockchain on internal control system components according to the COSO framework (Rückeshäuser, 2017; Bonsón & Bednárová, 2019; Schmitz & Leoni, 2019; Vincent & Barkhi, 2021).

Popchev et al. (2021), using blockchain technology, proposed a framework for the stages, procedures and elements for an internal audit plan in organizations implementing blockchain in smart crop production. The effects of blockchain technology on the features and functions of internal audit and internal control have been emphasized as a useful tool for internal controls and internal audit at the point of reducing and detecting risks (Popchev et al., 2021).

Blockchain has the potential to reduce or eliminate many risks associated with computer transactions. Many organizations have internal controls and processes for data backup. Diedrich (2016) emphasizes that with the blockchain, data is stored in a permanent registry and there will be no need for data backup anymore. When a violation occurs on a node, the remaining nodes will continue to operate as the entire registry, related protocols and source codes are available (Diedrich, 2016).

In addition to the studies emphasizing the advantages of using blockchain technology especially in the field of internal control and accounting, there are studies suggesting that it has disadvantages. In his study, Rückeshäuser (2017) argues that since blockchain-based accounting uses the majority of computer power, it is easier to circumvent internal and external control systems in this system compared to traditional accounting systems, and it paves the way for suspension of controls by management (Rückeshäuser, 2017). White et al. (2019) states that despite the attractiveness of Blockchain, like any new technology, it also carries a number of inherent risks. Inherent risks include technological risks affecting the assurance and audit function, data security risks, interoperability risks, and third-party supplier risks. Therefore, they stated that auditors should be prepared to assess inherent risks and consider its impact on the client, the environment, and internal controls (White et al., 2019).

Possible applications for the five components of the 2013 COSO Framework regarding the incorporation of blockchain technology into the business environment are discussed in detail in the following section.

3. Block Chain Technology and COSO Framework Components

COSO internal control model; It is a structure developed to create the organizational infrastructure necessary for the healthy execution of the activities of the components in interaction with each other, to successfully manage the risks that the enterprises face or to be exposed to, and to ensure the continuity and up-to-datedness of these processes. Explanations on internal control are included in the "Internal Control-Integrated Framework" COSO report. Internal control is a process designed to provide reasonable assurance to achieve the following business objectives affected by the board of directors, managers, and other personnel of the enterprise (Köse & Bekçi, 2017):

- Effectiveness and efficiency of activities,
- Reliability of financial reporting and
- Compliance with relevant laws and regulations

The 2013 COSO internal control framework (Table 3) includes the five components of internal control and 17 principles associated with these five components necessary for effective internal control.

Table 3. COSO's internal control: Integrated framework

Components	Principles
Control Environment	• Integrity and professional ethics • Surveillance responsibility investigations • Creation of task and authority distributions • Demonstrating commitment to competence • Authorities and responsibilities
Risk Assessment	• Setting appropriate goals • Identifying and analyzing risks • Assess fraud risk • Monitoring the changes that may occur in risks
Control Activities	• Selection and implementation of control activities • Implementation of technology-based general controls • Development of policies and processes
Information and Communication	• Using relevant information • Establishing internal communication • Establishing external communication
Monitoring	• Continuous monitoring activities and monitoring activities established when necessary • Evaluation of the lack of communication

Source:(Köse & Bekçi, 2017)

The emergence of the blockchain not only creates the need for new risks and new controls but also has the feature of being an effective tool for responding to existing risks and improving controls. At this point, the COSO 2013 Framework provides an effective and efficient approach that can be used to design and implement controls to address the unique risks associated with blockchain. Blockchain technology has the potential to significantly impact internal controls within organizations by aligning with various components of the COSO framework while introducing new aspects. The positive and negative effects of this technology on COSO components are presented in the Figure 1 (Özdemir & Mazak, 2021):

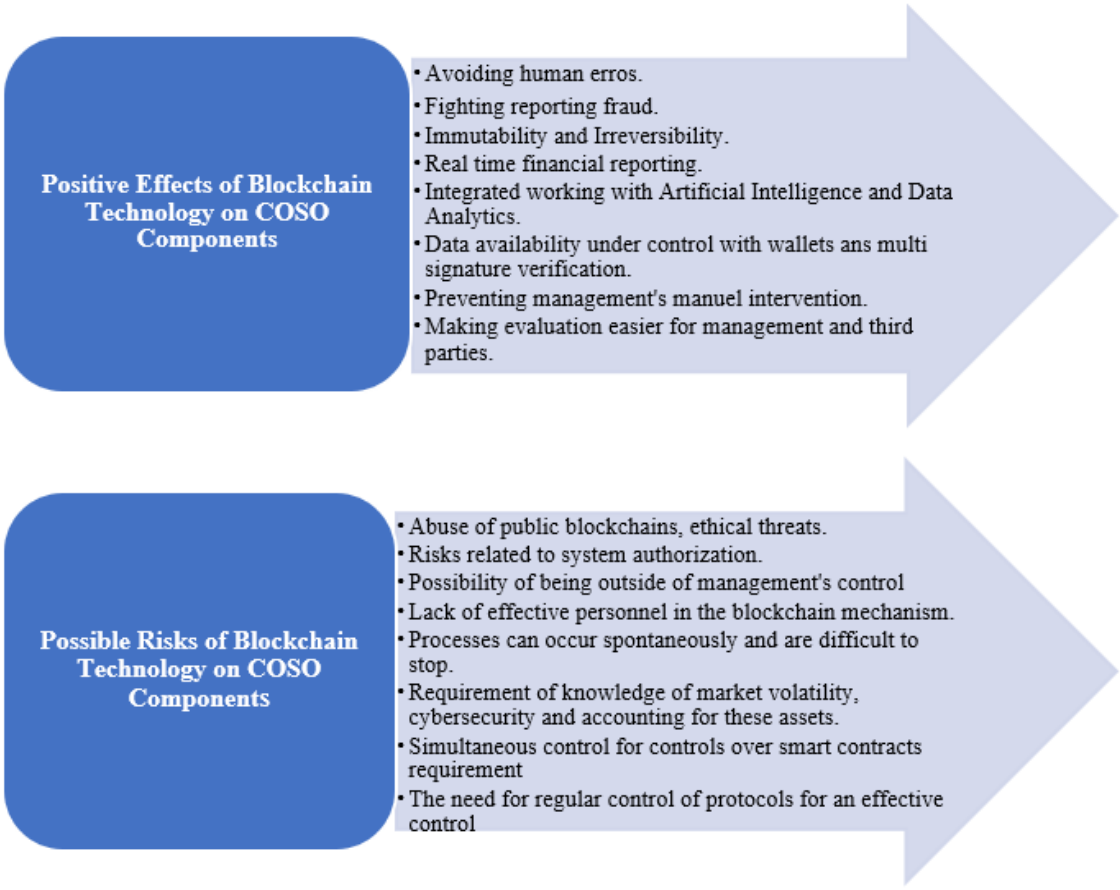

Figure 1. Advantages and risks of using blockchain

When implementing blockchain, the possible implications for internal controls over financial reporting should be analyzed, considering each of the 5 COSO components and 17 principles (Dickins & Fay, 2017).

3.1 Control Environment

The control environment, a foundational element of an organization's control architecture, encapsulates the policies and procedures that mirror the firm's ethos and attitude towards internal controls. This environment, propagated by management, creates an organizational milieu conducive for achieving broad and intricate business objectives. It is materialized through the implementation of procedures premised on high ethical standards, internal audit rules, and internal regulations. An efficacious control environment is typified by a competent organizational climate that exhibits an acute cognizance of its responsibilities and authority boundaries. This climate is marked by an intrinsic motivation to adhere to policies and procedures aimed at achieving business objectives (Riva & Provasi, 2015).

The control environment is influenced by the milieu in which the business operates. The internal control environment is an arena where employees can execute their activities and fulfill their responsibilities, thus providing a foundation for other control elements. In understanding the control environment, auditors strive to discern management's perceptions and attitudes towards controls. For instance, the presence and actualization of an effective budgeting system serve as pivotal indicators for auditors. The control environment is marked by the following elements, and an understanding of these is requisite for auditors. Blockchain technology can play an instrumental role in fostering a robust control environment (Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2013)).

The transparent and immutable attributes of blockchain technology can enhance the control environment by engendering a culture of honesty and trust. The decentralized characteristic of blockchain lessens dependency on intermediaries, thereby promoting a more transparent and accountable organizational culture.

The blockchain can augment the control environment by facilitating the execution and recording of transactions with minimal human intervention. The unique automation feature of the blockchain, coupled with the immutable nature of transaction ledgers, provides businesses with unique opportunities to prevent human errors and combat fraud. Blockchain imbues business processes with the capability to be cryptographically verified, immutable, and irreversible. The application of blockchain in these domains necessitates the development of internal controls to comply with the increasing regulations for financial data preparation. Simultaneously, stakeholders should adapt their risk-assessment policies and procedures, and audit committees should be equipped to address these challenges leading to financial statement preparation (Smith & Castonguay, 2020).

A well-designed and implemented blockchain engenders trust in processes and provides evidence. The utilization of blockchain supports the enterprise's commitment to integrity and ethical values, promoting transparency and accountability. In an internal control environment facilitated by blockchain, external auditors will encounter a more reliable audit environment.

Nevertheless, blockchain introduces certain risks. A poorly managed blockchain can be susceptible to abuse, particularly given the pseudo-anonymous nature of some blockchains. Decentralized blockchains exhibit a deficiency in accountability, a significant disadvantage concerning governance due to the absence of competent bodies to be held accountable for mishaps. Moreover, organizations associated with this technology may struggle to find competent personnel or to comprehend the technology fully.

Some of these risks can be mitigated by reinforcing adherence to ethical principles and developing a code of conduct for accountability. Organizations need to evaluate their capabilities and allocate appropriate internal or external resources to manage the technology effectively. It's crucial that the governance process is comprehended clearly, continually monitored, and evaluated for its effectiveness. Organizations could consider collaborating with an independent external expert to oversee system oversight and adherence. It is imperative that the independent external expert reports directly to the parties responsible for the organization's governance. Policies need to be developed to set guidelines and criteria to identify public blockchains for transactions (Burns et al., 2020).

3.2 Risk Assessment

The second component of internal control, risk assessment, pertains to the identification and analysis of risks, errors, and fraud that obstruct the fulfilment of business objectives. Rigorous efforts are required across the organization to detect, evaluate, and monitor events posing a threat to the realization of the organizational mission. Upon identification of risks, decisions must be made by management to either accept, mitigate to an acceptable level, or circumvent the risk entirely.

At all levels - macro, industry, enterprise, and project - organizations must detect and manage potential and existing risks. In addition to this, the assessment of the likelihood of risk occurrence and the extent of risk exposure should be undertaken. When applied effectively, risk assessment enables organizations to diminish the risk and likelihood of failure of new investments and projects through external oversight and internal corporate governance,

thereby identifying potential threats and reducing risk to an acceptable level (Chan et al., 2021).

The risk assessment process aims to draw attention to the most significant risks and opportunities, providing a comprehensive evaluation of risk magnitude, both collectively and individually, in response to threats. The efficacy of this process is contingent upon the right individuals possessing the required expertise, supported by appropriate technology, executing the assessment. By emphasizing a holistic perspective in risk estimation, the COSO risk assessment ensures that individuals can effectively fulfil their roles. An assessment process addressing each risk collectively and holistically enables an organization to manage its exposures effectively, identifying the appropriate types of risks to achieve its strategic objectives.

The inherent security features of blockchain can ameliorate certain risks associated with data tampering and fraud. The protection and auditability of data stored on a blockchain reduce the probability of unauthorized modification or manipulation, thereby positively influencing risk assessment.

The amalgamation of blockchain with other emergent technologies can facilitate real-time reporting to operations, the board, and external stakeholders, thus enabling a more effective risk assessment program that identifies and evaluates the achievement of diverse organizational objectives, whether operational, financial reporting, or compliance.

Risk identification and assessment in relation to objective achievement is an iterative process in the risk assessment phase. The incorporation of blockchain technology is likely to introduce new objectives and risks that necessitate consideration. It is vital to possess the relevant skills and resources to understand, continually identify, estimate, and address these new risks associated with blockchain.

While traditional risk assessments are centered around the protection of company assets, blockchain allows for a broader perspective of risk, particularly in relation to other parties in the blockchain network. For instance, organizations can evaluate the risk sensitivity of other parties in the blockchain network and its implications for their businesses. However, it should also be noted that new technology can heighten vulnerability to fraud, such as collusion. Furthermore, auditors may be impeded from obtaining valid evidence if the volume of data on the chain exceeds the organization's management capacity and transaction traces are lost electronically.

A more comprehensive risk assessment is necessary for organizations to consider the potential risks posed by blockchain technology. The involvement of IT professionals with expert knowledge of this technology can be beneficial in determining how it can be integrated into the existing structure of the organization. Such a risk assessment conducted prior to the implementation of blockchain technology also aids in evaluating the potential benefits and possible costs of the technology. Moreover, awareness of new regulations can be fostered by involving legal counsel and, importantly, internal audit (Burns et al., 2020).

3.3 Control Activities

Control activities, from a comprehensive perspective, encapsulate the policies and procedures established and enacted to address existing or emerging risks, and to achieve organizational objectives. These activities are not solely tied to maintaining operational continuity, but also involve the creation of regulations to ensure that organizational requirements are met as envisioned. Control activities thus form the backbone of an organization's internal control structure, enhancing its resilience and stability.

Such activities comprise policies that identify risk, facilitate the implementation of management decisions, and procedures developed by the individuals executing these policies. Control activities, designed to ensure tasks are performed correctly and efficiently, span both financial and non-financial domains and should be tailored to fit all organizational operations (Zhong, 2018).

Controls are primarily designed to ensure the execution of risk mitigation strategies within an organization. While some controls may be specific to certain areas, many have overlapping scopes. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) classifies control activities according to three primary organizational objectives (COSO, 2013):

1. Operations-related controls,
2. Financial reporting controls,
3. Compliance controls.

These controls can exist as standalone procedures or interlinked activities, often designed to mitigate multiple risks associated with more than one operational area. The key controls delineated by COSO, either manually operated or automated, include:

- Adequate segregation of duties,
- Appropriate authorizations for transactions and activities,
- Sufficient documentation and recording,
- Physical control over assets and records,
- Information technology application controls (encompassing input, processing, and output),
- Supervision of tasks performed by independent individuals (independent reconciliation).

Blockchain technology, when well-designed and implemented, can significantly enhance internal control

measures. The high degree of automation inherent to blockchain can provide a secure environment for mitigating traditional fraud risks by reducing manual intervention. Proper implementation of blockchain can help diminish threats linked to unauthorized access, alteration, or deletion of historical data.

Blockchain's cryptographic properties and its capacity to create smart contracts, coupled with its transparency, can serve as a powerful enabler for control activities. Its smart contract feature can automate various processes, approvals, and transactions, thereby minimizing manual intervention and associated errors.

By reducing manual intervention in the financial reporting process through the high degree of automation and the ability to verify and record immutable transactions in a common ledger, blockchain offers the potential to mitigate transactional and reporting frauds effectively. Consequently, opportunities for traditional fraud or manual error are reduced, and associated risks are likewise diminished.

Blockchain's capacity for near real-time transaction processing and recording can also help avoid timing errors, thus significantly reducing inaccuracies. However, the implementation of blockchain can have both positive and negative effects on an organization's internal controls. To maximize benefits and minimize risks, organizations need to address potential threats with new procedures, paying particular attention to critical aspects of blockchain such as nodes, consensus protocols, private keys, and smart contracts.

The reliability of a blockchain is contingent on the dependability of the underlying technology and business processes. A failed blockchain implementation or inadequate supporting controls could introduce new or exacerbate existing problems, including issues with smart contracts, key management, and consensus protocols.

To mitigate the risks associated with the implementation of blockchain and enhance the effectiveness of control activities, organizations should introduce policies and procedures pertaining to the use of blockchain. This will foster accountability for the system's operation. Crucial areas requiring development include nodes, consensus protocols, private keys, and controls over smart contracts (Burns et al., 2020).

Establishing controls for maintaining database copies, verifying transactions, preparing data for blockchain incorporation, and managing the activities of nodes providing other services is paramount. The design and auditing of consensus protocols should be conducted meticulously to ensure their effective operation.

Access to private keys should be restricted and controls relating to key storage should be stringent. An approach where access to the private key is divided among several parties could be considered. This would necessitate multi-signature validation by multiple parties for transactions. To ensure the appropriate segregation of duties, the organization should consider those who approve blockchain transactions separately from those who record transactions in the ledgers.

The efficient design and implementation of smart contracts is another area requiring attention. Controls should be applied to verify compliance at this point, changes and updates should be monitored in a controlled manner, and there should be appropriate documentation and historical records to ensure accountability.

3.4 Monitoring

Monitoring, a critical component of internal controls, is implemented to ascertain the efficacy and functionality of the internal control systems, including each component and policy. Given the dynamic nature of these systems and their implementation, it is imperative for management to perpetually assess the appropriateness of the internal controls and to continually identify emergent risks. This process, henceforth referred to as monitoring, facilitates the continuous improvement of internal control systems.

Monitoring involves the design of internal controls by appropriate personnel, the timely implementation of control actions, and the evaluation of the necessity of these actions. It should be noted that monitoring activities are applicable to each component of internal control. The internal audit unit or function serves as an instrumental monitoring tool, establishing a system of checks and balances. Controls exercised by the top level ought to be monitored by the top level, while risks that have evaded the attention of business management should fall under the scrutiny of the board of directors.

The advent of blockchain technology has introduced a dynamic element to the process of monitoring. Assessments can be developed in blockchain-enabled processes using smart contracts or artificial intelligence. Real-time data collection and analysis facilitate the capturing of issues closer to their occurrence, thereby enabling a timelier detection and resolution of these issues.

The transparency offered by blockchain technology allows for real-time monitoring of transactions. Auditors and internal control teams have access to comprehensive, tamper-proof records of transactions, thereby augmenting their ability to effectively monitor and evaluate controls.

However, potential risks may emerge with the application of blockchain technology. The storage of large volumes of data could result in an information overload, thereby complicating the monitoring process. Additionally, the recruitment of qualified personnel to establish and maintain an efficient monitoring system could present a challenge. The decentralized nature of the technology could further complicate the assignment of responsibility for monitoring. The rules governing blockchain could pose obstacles to the maintenance of monitoring-related changes.

Despite these challenges, the ability of blockchain to process large volumes of data and numerous transactions allows for the application of computer-assisted continuous monitoring techniques to perform ongoing assessments. These assessments can also ensure the functionality of internal controls and their compliance with regulations. Furthermore, the engagement of an external expert to evaluate the effectiveness of the internal controls could aid in the identification and escalation of system deficiencies and weaknesses to management. At this juncture, it is crucial for agreements with outsourced service providers to be closely monitored to safeguard the system's security and prevent the introduction of unreliable data (Burns et al., 2020).

4. Conclusions

Technological advancements incontrovertibly enhance the quality, precision, and efficacy of internal controls. In grappling with the risks associated with technology utilization, organizations are compelled to contemplate secure incorporation of technology into their internal control frameworks.

An assessment of blockchain's potential within the context of the COSO framework can equip business management with a comprehensive understanding of the issue. This understanding enables more informed evaluations of the technology's potential and applicability for internal control, and facilitates detailed risk analysis. Consequently, appropriate controls can be devised, harnessing the power of blockchain to address these risks effectively.

Blockchain technology fortifies organizations, particularly in the domain of transparency. It fosters knowledge sharing and simplifies the attainment of a single, real knowledge version. However, evolving company structures pose a challenge to the establishment of a standard structure that suits every company. The majority of companies are likely to adopt the system devoid of any assurance of preventive, detective, or corrective control for transaction creation, updating, and processing. The core question then arises: are existing frameworks, designed to approach risk and controls on a single-company basis, suitable in a multi-company blockchain and smart contract environment?

Capitalizing on the potential of blockchain necessitates addressing myriad challenges. It is anticipated that the resolution of these issues will be spearheaded by organizations and industries disrupted by blockchain, driven by the desire for transparent and accessible blockchain-based systems. These organizations will not only propel their own development but also cultivate novel use cases that enlighten others, including regulators and stakeholders, about blockchain's potential benefits.

The application of blockchain technology paves the way for the detection or prevention of deceptive financial reporting. Coupling blockchain with other technologies such as artificial intelligence, IoT, and machine learning can maximize the benefits specific to the reliability of financial reporting. Organizations can harness these distinctive features of blockchain to devise more robust and functional controls.

Future research avenues abound for exploring the impact of blockchain technology on internal controls under the COSO framework. Potential investigations could encompass in-depth case studies and empirical research scrutinizing how organizations integrate blockchain technology into their internal control systems. Further areas of inquiry might include the influence of blockchain technology on regulatory compliance and corporate governance practices, strategies and challenges associated with technology integration into existing IT systems and control environments, and the effect of smart contracts on control activities and process automation. Studies could also probe how blockchain technology might be employed to prevent and detect fraud, and how the COSO framework can evolve to incorporate blockchain-related aspects. The development of training materials and programs could enable professionals and practitioners to effectively comprehend and implement blockchain-enabled internal controls.

These potential research proposals underscore the interdisciplinary nature of the impact of blockchain technology on internal controls within the COSO framework. As technology and its applications continue to evolve, myriad opportunities await scholars, practitioners, and organizations to delve into and contribute to this rapidly evolving field.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

Bonsón, E., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari*

Account. Res., 27(5), 725-740. https://doi.org/10.1108/MEDAR-11-2018-0406
Burns, J., Steele, A., Cohen, E., & Ramamoorti, S. (2020). *Blockchain and ınternal control: The COSO perspective.* Committee of Sponsoring Organizations of the Treadway Commission, Durham.
Chan, K. C., Chen, Y., & Liu, B. (2021). The linear and non-linear effects of internal control and its five components on corporate innovation: Evidence from Chinese firms using the COSO framework. *Eur. Account. Rev.*, *30*(4), 733-765. https://doi.org/10.1080/09638180.2020.1776626
COSO. (2013). *Internal Control—Integrated Framework.* https://egrove.olemiss.edu/cgi/viewcontent.cgi?article=1769&context=aicpa_assoc.
Deloitte. (2020). *Blockchain and Internal Control: The COSO Perspective.* Committee of Sponsoring Organizations of the Treadway Commission, Durham.
Dickins, D., & Fay, R. G. (2017). COSO 2013: Aligning internal controls and principles. *Issues Account. Educ.*, *32*(3), 117-127. https://doi.org/10.2308/iace-51585
Diedrich, H. (2016). *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations.* Wildfire Publishing.
Köse, E. & Bekçi, İ. (2017). 1992-2013 COSO Modeli: İç kontrol-entegre çerçevesi. *Uluslararası Işletme, Ekonomi Yönet. Perspektif. Derg.*, *2*(7), 13-23. https://doi.org/10.20989/ijbemp.31
Koteska, B., Karafıloski, E., & Mishev, A. (2017). Blockchain implementation quality challenges: A literature. In *SQAMIA 2017: 6th workshop of software quality, analysis, monitoring, improvement, and applications*. Belgrade, Serbia, pp. 8. https://ceur-ws.org/Vol-1938/paper-kot.pdf.
Lim, S. (2023). *Blockchain: The COSO perspective.* https://medium.com/@sharonlimty/blockchain-the-coso-perspective-part-1-2-293f41eab6b4.
Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. Curr. *Issues Audit.*, *13*(2), A19-A29. https://doi.org/10.2308/ciia-52540
Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Bus. Inf. Syst. Eng.*, *59*, 183-187. https://doi.org/10.1007/s12599-017-0467-3
Özdemir, O. & Mazak, M. (2021). Blokzincir Teknolojisi ve iç kontrol sisteminin yeniden yapılandırılması: COSO bileşenleri üzerinden bir değerlendirme. In *Denetimde Seçme Konular 8: İç Kontrol İç Denetim.* (pp. 85-110). Gazi Kitabevi, Türkiye.
Popchev, I., Radeva, I., & Velichkova, V. (2021). The impact of blockchain on internal audit. In *2021 Big Data, Knowledge and Control Systems Engineering (BdKCSE). Sofia, Bulgaria.* (pp. 1-8). Sofia, Bulgaria. https://doi.org/10.1109/BdKCSE53180.2021.9627276
PricewaterhouseCoopers. (2019). *Re-inventing internal controls in the digital age.* https://www.pwc.com/sg/en/publications/assets/reinventing-internal-controls-in-the-digital-age-201904. pdf.
Riva, P. & Provasi, R. (2015). The updated COSO report 2013. *J. Mod. Account. Audit.*, *11*(10), 487-498. https://dx.doi.org/10.17265/1548-6583/2015.10.001
Rückeshäuser, N. (2017). Do we really want blockchain-based accounting? Decentralized consensus as enabler of management override of internal controls. In *International Association for Information Systems and Economics 2017.* (pp. 16-30). St. Gallen, Switzerland. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1001&context=wi2017.
Schmitz, J. & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: A research agenda. *Aust. Account. Rev.*, *29*(2), 331-342. https://doi.org/10.1111/auar.12286
Smith, S. S. (2020). Internal control considerations. In *Blockchain, Artificial Intelligence and Financial Services* (pp. 143–150). Springer International Publishing. https://doi.org/10.1007/978-3-030-29761-9_11
Smith, S. S., & Castonguay, J. J. (2020). Blockchain and accounting governance: Emerging issues and considerations for accounting and assurance professionals. *J. Emerg. Tech. Account.*, *17*(1), 119-131. https://doi.org/10.2308/jeta-52686
Tadesse, A. F., Rosa, R. C., & Park, R. J. (2022). The adoption and consequences of COSO 2013. *Account. Horiz.*, *36*(4), 241-260. https://doi.org/10.2308/horizons-18-123
Vincent, N. E., & Barkhi, R. (2021). Evaluating blockchain using COSO. *Curr. Issues Audit.*, *15*(1), A57-A71. https://doi.org/10.2308/CIIA-2019-509
White, B. S., Holladay, J., & King, C. G. (2019). Blockchain security risk assessment and the auditor. *J. Corp. Account. Fin.*, *31*(2), 47-53. https://doi.org/10.1002/jcaf.22433
Zhong, R. I. (2018). Transparency and firm ınnovation. *J. Account. Econ.*, *66*(1), 67-93. https://doi.org/10.1016/j.jacceco.2018.02.001