International Journal of Auditing and Accounting Studies
ISSN: 2582-3272 • Volume 6; Number 3; 2024 : pp. 401-423
https://DOI:10.47509/IJAAS.2024.v06i03.06

ARF INDIA
Academic Open Access Publishing
www.arfjournals.com

ENHANCING INTERNAL CONTROLS FOR SMART CONTRACTS: A COMPREHENSIVE FRAMEWORK FOR BLOCKCHAIN

Sara Beshir[1] Ismail Gomaa[2] Otake Toshitsugu[3] and Hosam Moubarak[4] Hebatallah A. Badawy[5]

[1]Faculty of International Business and Humanities, Egypt-Japan University of Science and Technology, Alexandria, Egypt. E-mail: sara.beshir@ejust.edu.eg
[2]Faculty of International Business and Humanities, Egypt-Japan University of Science and Technology, Alexandria, Egypt. E-mail: ismail.gomaa@ejust.edu.eg
[3]College of International Management, Ritsumeikan Asia Pacific University, Beppu, Japan. E-mail: totake@apu.ac.jp
[4]Faculty of International Business and Humanities, Egypt-Japan University of Science and Technology, Alexandria. E-mail: hosam.moubarak@ejust.edu.eg
[5]Faculty of International Business and Humanities, Egypt-Japan University of Science and Technology, Alexandria. E-mail: heba.badawy@ejust.edu.eg

Received: 2 May 2024: Revised: 10 and 14 July 2024: Accepted: 20 July 2024 : 28 October 2024

Abstract: This research presents a novel approach to enhancing internal controls for smart contracts in the context of blockchain technology. The groundbreaking integration of blockchain technology and smart contracts into various industries has been driven by the extensive research conducted in Accounting Information Systems (AIS). However, it is crucial to have robust internal control systems to effectively mitigate the security risks and confidentiality concerns associated with smart contracts. As such, this paper stands out as one of the first initiatives to integrate more than two frameworks for internal controls, such as COSO and COBIT. This study introduces a comprehensive framework that institutions can utilize to empower blockchain users to enhance the internal controls for smart contracts. Our findings recommend integrating multiple frameworks to bolster the governance of smart contracts. Furthermore, we emphasize the need for continuous updates and dynamic adaptation within the framework. A structured process for regular review and adjustment of framework components ensures alignment with evolving regulatory requirements and emerging technological advancements in blockchain. This research leveraged a combination of frameworks and collected data from 205 blockchain experts. The data was then analysed using the explanatory factor analysis that validated the factor structure, confirming strong factor loadings, composite reliability, and average

To cite this paper:
Sara Beshir, Ismail Gomaa, Otake Toshitsugu, Hosam Moubarak and Hebatallah A. Badawy. (2024). Enhancing Internal Controls for Smart Contracts: A Comprehensive Framework for Blockchain. *International Journal of Auditing and Accounting Studies*. 6(3), 401-423. *https://DOI:10.47509/IJAAS.2024.v06i03.06*

variance extracted (AVE) for each latent variable, and confirmatory factor analysis methods to validate the framework satisfactory model fit indices. The integration of diverse frameworks not only addresses challenges but also encourages professionals to explore and experiment with these transformative technologies.

Keywords*:* Smart Contracts; Internal Controls; Integrated Frameworks; Security; Blockchain Internal Controls.

1. INTRODUCTION

In recent years, accounting, auditing, and accountability fields have been significantly revolutionized, driven by technological advancements (Kalyani & Murugan, 2021). One of the most influential technologies that have emerged during this period is blockchain, which has brought forth both challenges and opportunities for professionals in accounting and auditing. Blockchain initiatives are increasingly using various Distributed Ledger Technology (DLT) platforms and providers, including Ethereum, Corda, and Hyperledger. This innovative technology, acting as both an application and a database, is fundamentally changing the way multiple industries operate. At its core, blockchain is a decentralized ledger system used to securely record transactions across multiple computers (Vincent & Barkhi, 2021). The potential of blockchain extends to diverse industries, offering enhanced transparency and security for applications such as elections and public record management (Jansiti & Lakhani, 2017; Queiroz et al., 2020). These transformative technologies drive innovation and prompt a reimagining of traditional business models, compelling organizations to explore their integration actively.

Smart contracts are a crucial aspect of blockchain technology. They are also known as self-executing, digital, or blockchain contracts that transform traditional contracts into computer codes, which are then stored and replicated across the system (Narayanan et al., 2016). A network of computers supervises these codes and enables the transparent exchange of money, property, shares, or other assets. In short, smart contracts' computer codes automatically execute a transaction when the program autonomously verifies the fulfillment of specific conditions securely recorded by the decentralized ledger. This facilitates the transaction in an immutable, tamper-proof manner, ensuring security and validity (Mougayar & Buterin, 2016), and allows the program to determine the redistribution of assets among the involved parties (Lu et al., 2018).

The traditional internal control frameworks are specifically designed to evaluate governance, management, internal controls, and interactions with external entities from the perspective of a single company. As a result, companies find it necessary to verify that all participants are following these established governance mechanisms and internal controls. This verification process is essential to ensuring the trustworthiness of the decentralized blockchain ledger, which includes smart contracts, as an accurate accounting record (Doekhi, 2023).

The objective of our research is to develop a comprehensive framework to improve the internal controls of smart contracts by integrating several frameworks, such as COSO, COBIT, ITIL, and NIST. Each framework has its own strengths in addressing various aspects of governance, risk management, and compliance. COSO's Internal Control—Integrated Framework provides a strong structure for risk assessment and control activities, which is critical for ensuring the secure execution of smart contracts (Vincent & Barkhi, 2021). COBIT helps align IT processes with business objectives to ensure that the implementation of smart contracts supports organizational goals. ITIL focuses on IT service management, which is important for ensuring efficient and reliable IT services to support smart contract performance. Lastly, NIST offers detailed guidelines for cryptographic controls and access management, which can enhance the security and compliance of smart contracts (Ettish et al., 2017). Integrating these frameworks into a comprehensive framework will help in mitigating risks, ensuring compliance, and supporting the efficient operation of smart contracts.

The remainder of this paper is structured as follows: Section 2 analyzes the literature review related to smart contract internal controls. Section 3 proposes a comprehensive framework for smart contract internal controls. Section 4 describes the benefits and implementation guidance. Section 5 presents the methodology and results. Section 6 discusses the evaluation of blockchain smart contracts, and Section 7 concludes the paper and recommends future research avenues.

2. LITERATURE REVIEW

2.1. Challenges in smart contract internal controls

Smart contracts are a powerful feature of blockchain technology, offering a wide range of benefits. They serve as efficient tools for automating tasks and ensuring secure and transparent transactions. Smart contracts are digital agreements designed to automatically execute the terms of a contract between the buyer and seller in a streamlined process, which in turn eliminates the need for intermediaries. One of the key advantages of smart contracts is their ability to provide a clear audit trial, which can be valuable for future reference (Tapscott & Tapscott, 2016). By automating processes, smart contracts not only enhance efficiency of transactions and business operations but also reduce the risk of errors that often occur with manual processing, thus improving accuracy. Furthermore, these powerful tools demonstrate their adaptability and versatility through a variety of applications, ranging from financial services to supply chain management (Khan et al., 2021). However, businesses must be aware of the specific challenges and risks associated with smart contracts. This section delves into these challenges and emphasizes potential vulnerabilities, security risks, and problems with legal compliance (Tschorsh & Scheuermann, 2016; Ellul et al., 2020).

Given that smart contracts are essentially programs written in code, they are susceptible to the same bugs and vulnerabilities as other software. Malicious parties could potentially exploit these mistakes to gain unauthorized access or cause financial losses. As a result, maintaining the integrity of smart contracts is crucial (Singh et al., 2019; Ellul et al., 2020). Although the security of blockchain is robust, it is not impervious to threats. Smart contract execution may be hindered by security flaws such as Distributed Denial of Service (DDoS) attacks. Additionally, off-chain components of smart contracts, like oracles, may be vulnerable to security risks (Conti et al., 2018). The legal environment surrounding smart contracts can be complex, as the absence of clear legislation in many jurisdictions may lead to uncertainty regarding organizations' legal responsibilities. As such, it is essential for businesses to navigate these challenges and ensure the proper management of smart contracts to harness their full potential while mitigating the associated risks (Budayan and Okudan, 2023).

Smart contracts involving sensitive data or financial transactions must comply with existing laws, such as data protection and financial rules (Bayon, 2019; Taherdoost, 2023). Once implemented, smart contracts become immutable, making it difficult to modify them. Any mistakes or changes in business requirements may necessitate a complete rewrite of the smart contract (Kosba et al., 2016; Zhang et al., 2016). Despite code audits and rigorous testing, human error, including misconfiguration of contract parameters, mistaken transactions, or bugs in the contract's code (Budayan & Okudan, 2023), observable during development could have significant consequences (Atzei et al., 2017).

As blockchain networks expand, scalability becomes a concern. Smart contract execution can be delayed due to network congestion, reducing effectiveness and usability (Casey & Vigna, 2018; Sheldon, 2019).

Incompatibility between different blockchains and smart contract platforms presents a technical challenge in achieving interoperability (Iansiti & Lakhani, 2017). To address these challenges, a comprehensive approach to internal controls and risk management must be adopted. This approach includes conducting thorough code audits, implementing security best practices, and keeping up with evolving legal frameworks (Sreejith & Senthil, 2023). Additionally, continuous monitoring and assessments are crucial for identifying and mitigating risks associated with blockchain-based smart contracts (Brender et al., 2023). In short, smart contracts are prone to security risks due to their code-based nature, especially if not properly designed and tested (Khan et al., 2021). Furthermore, the legality of smart contracts is still questionable because of their legal enforceability, jurisdiction, and compliance with existing laws (Taherdoost, 2023). Technical challenges such as scalability, costs, and integration with traditional systems also present hurdles to their widespread adoption.

In 2016, 'The DAO' a decentralized autonomous organization on the Ethereum blockchain fell victim to a critical flaw in its smart contract code. Exploiting this vulnerability, an attacker took advantage of this weakness of approximately 3.6 million Ether, valued at over $50 million at that time. This incident underscored the importance of auditing, code reviews, and vital internal controls for smart contracts (Popper, 2016; Morrison et al., 2020). Moreover, several crypto currency exchanges operating on smart contracts have also grappled with security breaches and internal control deficiencies, leading to the loss of user funds and reducing confidence in the crypto ecosystem (Kim & Lee, 2023; Lee & Wie, 2023). The likelihood of such breaches on these exchanges could have significantly been mitigated by implementing risk management practices, improving security measures, and conducting regular assessments and evaluations, safeguarding both their assets and user interests. While the decentralized finance (DeFi) industry has experienced rapid growth, it has also faced difficulties in regulatory compliance. Some DeFi projects have faced legal hurdles related to offering unregistered securities or facilitating money laundering (Crenshaw, 2021).

Notably, there is a lack of comprehensive literature specifically addressing the integration of COSO, COBIT, ITIL, and NIST frameworks to enhance internal controls for smart contracts. Although each of these frameworks individually contributes to governance, risk management, IT service management, and cybersecurity, there is insufficient research on their combined application to address the unique challenges of smart contracts. For instance, COBIT 2019 provides a detailed model for IT governance (Nachrowi et al., 2020), and NIST offers critical infrastructure cybersecurity improvements (NIST,2018). However, the literature does not extensively cover how these can be harmonized to fully secure and govern smart contracts. This indicates the necessity for further research and the development of a unified framework that harnesses the strengths of these established standards to effectively manage and control the complexities inherent in smart contract technology. Smart contracts' complexity and automated execution increase operational risks and vulnerabilities. There is a gap in ensuring the reliability and auditability of smart contracts, hindering trust and accountability (Hasan et al., 2023). Existing frameworks lack adequate decentralized access control mechanisms, exposing vulnerabilities (Rozario & Thomas, 2019). To address these gaps and challenges, a new framework should integrate governance by design, enhance audit procedures with blockchain support, and implement robust access control protocols. Such advancements are crucial to fostering trust, improving security, and ensuring the reliability of smart contracts in blockchain ecosystems.

2.2. Importance of internal controls in smart contracts

Internal controls are crucial in the realm of blockchain-based smart contracts as they provide a solid foundation for ensuring reliability, security, and compliance within the context of smart contracts (Tapscott & Tapscott, 2016). This section highlights the vital role of internal controls in reducing risks, enhancing security, and guaranteeing adherence to regulatory compliance. Smart contracts automate numerous processes, ranging from financial transactions to supply chain management; however, these procedures are not risk-free. Despite the inherent security benefits of blockchain technology, smart contracts are vulnerable to exploitation by malicious actors and external threats. As such, internal controls serve as protective mechanisms that enforce access restrictions, encryption, and audit trails, thereby strengthening security measures and creating a multi-layered defense system to safeguard the integrity and privacy of smart contract data (Marko & Kostal, 2022). This leads to identifying and managing potential risks, aiding in risk assessments, and assisting businesses in addressing vulnerabilities effectively (Marko & Kostal, 2022).

Emphasizing the continuously evolving regulatory environment governing smart contracts, internal controls play a critical role in ensuring compliance with pertinent laws and standards, enabling organizations to navigate this complex terrain. Organizations can demonstrate their adherence to legal obligations and reduce the risk of penalties or legal disputes by documenting processes, transactions, and compliance efforts (Tapscott & Tapscott, 2016). Additionally, internal controls create mechanisms for identifying and preventing fraudulent activity within smart contracts. Organizations can significantly lower the risk of fraudulent transactions or activities by implementing segregation of duties, dual authorization, and transaction verification controls (Zheng et al., 2022). Moreover, effective internal controls enhance transparency by providing a record of all actions within the smart contract, fostering trust, and simplifying dispute resolution (Tapscott & Tapscott, 2016). They also streamline operations and automate processes, reducing the need for manual oversight to minimize the risk of human error in contract execution while improving efficiency.

On the other hand, assessing the internal controls of smart contracts can be challenging as a result of the complexity of technology and the new risks it introduces. However, various frameworks can be used to assess the internal controls of blockchain-based smart contracts, address potential issues, and enhance overall security (Tapscott & Tapscott, 2016). To address these challenges, this paper proposes an essential comprehensive framework for robust internal controls in smart contracts. Such a framework focuses on enhancing security, clarifying legal aspects, overcoming technical limitations, and ultimately facilitating broader adoption of smart contracts.

2.3. Exploring framework contributions and limitations

In this section, we delve into the unique contributions and potential limitations of selected frameworks—COSO, COBIT, ITIL, and the NIST Cybersecurity Framework—pertaining to the intricacies of smart contracts within the blockchain ecosystem. Our goal is to analyze the principles of these frameworks and create a comprehensive and adaptable framework to address the specific challenges posed by smart contracts in the blockchain environment.

First, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides a practical approach to designing and implementing controls for blockchain-related risks. As blockchain gains wider adoption, it is essential to consider how it intersects with an entity's internal control. Leveraging COSO's Internal Control—Integrated Framework (COSO, 2017) allows organizations to conduct a detailed risk analysis and establish control activities tailored to address blockchain-specific risks. However, it is important to note that COSO's framework is not explicitly tailored to blockchain technology and lacks detailed technical guidance for smart contract implementation (Vincent & Barkhi, 2021).

Second, the National Institute of Standards and Technology (NIST) offers guidelines for secure software development and risk management, focusing on cryptographic controls, access management, and regulatory compliance. These guidelines align well with the security challenges of smart contracts in the context of blockchain technology. By incorporating NIST's recommendations, organizations can enhance the security posture of their smart contracts and protect against vulnerabilities and unauthorized access. However, it is worth mentioning that NIST documents can be highly technical and require expertise for effective implementation (NIST, 2018; Khan et al., 2021).

Third, the Control Objective for Information and Related Technology (COBIT) emphasizes the importance of aligning IT with business goals. Clearly defined objectives related to smart contracts are essential, and integrating COBIT's governance principles with other frameworks can help create a holistic approach to internal controls. However, COBIT is not a blockchain-specific framework and requires adaptation to address the unique risks associated with smart contracts (ISACA, 2019; Xu et al., 2021; Taherdoost, 2023; Kamil et al., 2023).

Lastly, the Information Technology Infrastructure Library (ITIL) is a framework for IT service management that can be utilized to ensure that the development and deployment of smart contracts align with the organization's overall IT service management strategy (Gevalla et al., 2018).

To effectively address the complexities of smart contracts in blockchain ecosystems, a comprehensive framework is necessary. Such a framework should blend the risk management rigor of COSO, the security-centric approach of NIST, the governance principles of COBIT, and the operational efficiency insights from ITIL. By synthesizing these frameworks, organizations can develop a holistic approach to managing smart contract risks, ensuring compliance, and optimizing operational performance within blockchain environments. This comprehensive framework would provide clear guidance tailored specifically to the unique challenges and opportunities presented by smart contracts on blockchain platforms.

3. DEVELOPMENT OF A COMPREHENSIVE FRAMEWORK OF SMART CONTRACT CONTROLS

In the following section, we present a comprehensive framework that has been meticulously designed, as shown in Figure 1, to strengthen the internal controls of smart contracts built on blockchain technology. This framework encompasses essential components, fundamental principles, control activities, and relevant frameworks, all aimed at ensuring smart contracts' security, reliability, and compliance.

The scope of this comprehensive testing framework encompasses the assessment of internal controls within smart contracts operating on blockchain platforms. The framework is designed to address various dimensions of control, risk management, security, and compliance associated with the deployment, execution, and ongoing maintenance of these smart contracts. The testing will be focused on identifying vulnerabilities, evaluating the effectiveness of controls, and ensuring alignment with relevant industry standards and regulations.

The objectives of this comprehensive testing framework are multifaceted. Firstly, it plays a crucial role in ensuring that smart contracts are constructed to meet certain conditions, such as the accuracy, reliability, and security of data and transactions. This construction is done in a manner that guarantees trustworthiness and accountability, instilling confidence in the system. Additionally, the framework strives to uncover vulnerabilities, exposure, and issues inherent in the design, coding, and functioning of smart contracts on blockchain networks. Moreover, it seeks to identify, prioritize, and provide recommendations for mitigating risks associated with executing smart contracts using blockchain platforms and ensure compliance with industry regulations, standards, and frameworks like COSO, COBIT, ITIL, and NIST Cybersecurity Framework. The proposed framework is designed to work in tandem with these existing frameworks, enhancing their effectiveness and addressing the unique challenges of smart contracts in the blockchain environment.

The framework plays a crucial role in evaluating the existing security measures in place to safeguard smart contract information, such as privacy, integrity, availability, and authorization. It also provides structured procedures to assess the traceability and auditability of smart contract transactions, ensuring proper accountability and transparency. Moreover, it offers significant recommendations to enhance the efficiency of internal controls, security mechanisms, and risk management procedures within the smart contract processes. The framework is also instrumental in assessing the ability of smart contracts and blockchain infrastructure to withstand disruptive challenges and ensure continuous business operations. By implementing this framework, organizations can significantly enhance the security, reliability, and compliance of their smart contracts, thereby reducing the risk of fraud, legal disputes, and non-compliance.

The foundation for ongoing monitoring, testing, and improvement of smart contract processes is established on the principles of ITIL and other relevant standards. These frameworks are not just about ensuring compliance, but also about instilling confidence in stakeholders, including management, auditors, regulators, and customers, regarding the appropriateness of the internal controls for smart contracts and their effective functionality. The active involvement and collaboration of these stakeholders are crucial for the successful implementation and maintenance of the framework. The framework not only provides decision-makers with insight into the reliability of smart contracts but also enhances staff's knowledge of internal control procedures, safety measures, and risk reduction techniques. It fosters cross-department cooperation, involving legal, compliance, audit, and IT, to gain a comprehensive understanding of smart contract testing and risk management. A detailed guideline for all principles laid out in the framework is provided in Appendix 1.

4. IMPLEMENTATION GUIDANCE

4.1. Practical steps for effective implementation

Implementing the framework for enhancing internal controls in smart contracts on the blockchain necessitates a structured approach to ensure its effectiveness (figure 1). The process begins with comparing the current state of internal controls within smart contracts with the practical steps and best practices, which in turn helps identify the controls' strengths, weaknesses, and gaps within the organization's strategic objectives and industry-specific requirements. This also involves insights from various stakeholders during the implementation process, including legal experts, IT professionals, compliance officers, and blockchain specialists. It is also critical to well-train teams on implementing the framework and ensure that all individuals involved understand their roles and responsibilities.

Leveraging technology, especially blockchain-based solutions and technologies can facilitate control activities by utilizing the inherent features of blockchain, such as immutability and transparency. Organizations should implement continuous monitoring, which is essential to ensure that controls are functioning as intended, and the framework should be regularly reviewed and updated to adapt to technological and regulatory changes. This involves establishing robust audit and reporting procedures, including regular internal audits, which is essential to evaluate the control effectiveness and maintain clear records of audit results. It is also crucial for organizations to stay informed about legal and regulatory changes in their jurisdiction to ensure continuous compliance with applicable laws and standards. Keeping in mind organizations

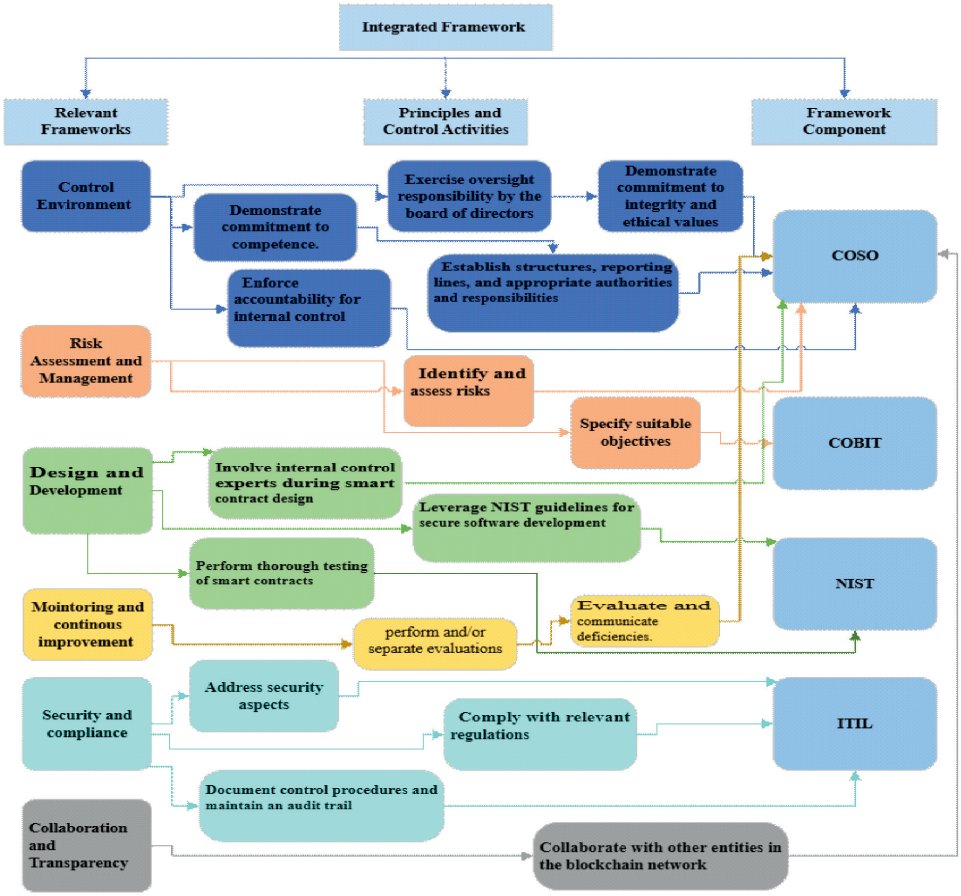
Integrated Framework
Relevant Frameworks
Principles and Control Activities
Framework Component
Control Environment
Demonstrate commitment to competence.
Exercise oversight responsibility by the board of directors
Demonstrate commitment to integrity and ethical values
Enforce accountability for internal control
Establish structures, reporting lines, and appropriate authorities and responsibilities
COSO
Risk Assessment and Management
Identify and assess risks
Specify suitable objectives
COBIT
Design and Development
Involve internal control experts during smart contract design
Leverage NIST guidelines for secure software development
Perform thorough testing of smart contracts
NIST
Mointoring and continous improvement
perform and/or separate evaluations
Evaluate and communicate deficiencies.
Security and compliance
Address security aspects
Comply with relevant regulations
ITIL
Document control procedures and maintain an audit trail
Collaboration and Transparency
Collaborate with other entities in the blockchain network

Figure 1: Theoretical comprehensive framework to enhance the smart contract internal controls.

Source: Authors' own work

must seek independent external expertise to provide impartial assessments of the control environment.

Furthermore, maintaining comprehensive documentation of all control activities, risk assessment procedures, and audit findings is essential to ensure transparency, compliance, and future improvements. Fostering a culture of employee awareness and encouraging employees to report potential weaknesses or security concerns is also vital. In these terms, organizations should continuously refine the control environment based on insights from audits and incidents while staying informed about emerging blockchain technologies and trends to adapt the framework accordingly. By integrating these structured steps and best practices into the implementation plan, organizations can effectively enhance internal controls for smart contracts on the blockchain, ensuring security, compliance, and optimized smart contract operations.

5. RESEARCH METHODOLOGY

5.1. Research design

The research used a survey-based method that covered framework variables and four demographic questions. A comprehensive questionnaire comprising 24 questions was administered by Google Form and sent to the respondents to gather data. Participants were directed to an online questionnaire, where they were provided with informed consent to analyze their data according to the outlined study's objective. In responding to this questionnaire, participants used a Likert-type scale with five levels: "strongly disagree," "disagree," "neutral," "agree," and "strongly agree.".

5.2. Participants selection and data collection

A total of 238 blockchain experts were specifically chosen and invited through professional networking platforms, such as LinkedIn and email, to participate in the research. The collected data was analyzed using the statistical software SPSS26.0 and AMOS23.0. The data collection phase lasted for 45 days. We sent out 400 questionnaires, and out of the 238 responses received (a response rate of 59%), only 205 responses were identified as valid after conducting the validation process to address incomplete or erroneous data entries. Based on the demographic data analysis (Table 1), it is evident that a significant proportion of the respondents identify as male, accounting for 85.9% of the total. Additionally, the data indicates that 59% of the respondents are over 30 years old, and 56.6% hold a bachelor's degree. Moreover, the analysis also encompassed a range of different analyses such as a reliability test, exploratory factor analysis (EFA), and confirmatory factor analysis (CFA).

Most respondents (85.9%) identified as male, while only 14.1% identified as female. This disparity suggests a predominance of male participants in the blockchain expert community. 20 under 30: 41% of respondents fall into this age group, indicating a significant presence of younger professionals in the field. Over 30: 59% of respondents are over 30 years old, reflecting a substantial portion of more experienced individuals in the blockchain sector. The largest educational group, comprising 56.6% of respondents, indicates a strong representation of individuals with undergraduate education. 34.6% hold a master's degree, and 8.8% have a Doctoral degree, showcasing a well-educated cohort in the blockchain domain

The data reveals that a significant portion of respondents, 49.8%, have 1-3 years of experience in using smart contracts. This indicates that many users are relatively new to the technology but have surpassed the initial learning phase. The next largest group, comprising 33.2% of respondents, has 4-6 years of experience, suggesting a solid familiarity and more advanced understanding of smart contracts. A smaller segment, 5.9%, has 7-10 years of experience, indicating a high level of expertise and long-term involvement in the field. Finally, 11.2% of respondents have less than 1 year of experience, representing newcomers to smart contracts. This distribution suggests a robust and growing user base with a diverse range of experience levels, highlighting both the technology's increasing adoption and the continuous influx of new users.

Table 1: Demographic Data

Item	*Category*	*Number of Respondents*	*Percent*
Gender	Male	176	85.9
	Female	29	14.1
	Total	205	100
Age	20 under 30	84	41
	Over 30	121	59
	Total	205	100
Education Level	Doctoral	18	8.8
	Masters	71	34.6
	Bachelor	116	56.6
	Total	205	100
Years of experience using smart contracts	Less than 1 year	23	11.0
	1-3	103	49.8
	4-6	68	33.2
	7-10	12	5.9
	Total	205	100

6. RESULTS

6.1. Descriptive Statistics

Table 2 presents descriptive statistics. It provides insights into seven variables: DDAVG, CEAVG, RAAVG, MAVG, SCAVG, CTAVG, and ICAVG, each calculated from a sample size of 205 respondents. CEAVG exhibits the highest mean (18.3883) and the greatest variability (SD = 2.11842), suggesting a wide range of responses. In contrast, DDAVG shows the lowest mean (6.5244) and the least variability (SD = 1.05226), indicating more consistent responses. Other variables, such as MAVG, SCAVG, CTAVG, and ICAVG, have similar means around 10 with moderate variability, suggesting a consistent central tendency with some spread in responses. The ranges also vary, with CEAVG spanning from 7.40 to 21.00 and CTAVG having the broadest range (3.33 to 11.67). This analysis highlights the diversity and consistency in respondents' perceptions across different constructs, with CEAVG showing the most significant spread and DDAVG the least.

Table 2: Descriptive Statistics

	N	*Minimum*	*Maximum*	*Mean*	*Std. Deviation*
DDAVG	205	2.50	7.50	6.5244	1.05226
CEAVG	205	7.40	21.00	18.3883	2.11842
RAAVG	205	7.00	16.25	14.2134	1.73325
MAVG	205	4.67	11.67	10.1203	1.35828
SCAVG	205	4.00	11.67	10.1593	1.34738
CTAVG	205	3.33	11.67	10.0780	1.45011
ICAVG	205	4.00	11.67	10.0878	1.35356
Valid N (listwise)	205				

6.2. Reliability Analysis

The reliability of the questionnaire was assessed using Cronbach's alpha coefficient, focusing on the 20 questions related to the multiple aspects of the framework, including control environment, risk assessment and management, design and development, monitoring and continuous improvements, security and compliance, and finally, collaboration and transparency. According to Kannan and Tan (2015), a Cronbach's alpha coefficient of 0.7 or higher indicates good reliability. Table 3 reveals Cronbach's alpha for each construct. High Cronbach's alpha values indicate strong internal consistency among the survey questions.

Table 3: Reliability analysis

Construct	*Cronbach's alpha*	*No. of questions*
Control Environment	0.810	5
Risk Assessment and Management	0.803	4
Design and Development	0.990	2
Monitoring and continuous improvements	0.841	3
Security and Compliance	0.764	3
Collaboration and transparency	0.888	3
Total		20

6.3. Exploratory factor analysis (EFA)

In order to identify the underlying factor structure (Hosain et al., 2021), an exploratory factor analysis (EFA) was conducted in this study. Taking the existence of several assumptions into account, including Kaiser-Meyer-Olkin (KMO) measure greater than 0.5, and that Bartlett's Test of Sphericity was significant ($p < 0.001$), indicating the suitability of data for factor analysis, having each factor with minimum loading of 0.50, and sample size considerations.

Upon conducting the EFA, as shown in Table 4, we found that all variables had a factor loading greater than 0.50. Additionally, we assessed the composite reliability of all variables, ensuring that they all met the minimum level of 0.7, as outlined by Bari et al. (2016). Thus, the identified factors are proven to be statistically significant and relevant for data analysis.

Table 4: Exploratory factor analysis

Latent variable	*Item*	*Factor load*	*Composite Reliability*	*Average Variance Extracted (AVE)*
Control Environment	CV1	0.827	0.918	0.692
	CV2	0.706		
	CV3	0.888		
	CV4	0.873		
	CV5	0.852		
Risk Assessment and Management	RA1	0.886	0.912	0.721
	RA2	0.874		
	RA3	0.828		
	RA4	0.806		
Monitoring and continuous improvements	MC1	0.800	0.910	0.772
	MC2	0.913		
	MC3	0.918		
Security and compliance	SC1	0.908	0.913	0.778
	SC2	0.838		
	SC3	0.899		
Design and Development	DD1	0.918	0.723	0.566
	DD2	0925		
Collaboration and transparency	CT1	0.918	0.940	0.840
	CT2	0.913		
	CT3	0.918		

6.4. Conformity Factor Analysis (CFA)

Confirmatory Factor Analysis (CFA) is a statistical method used to validate the factor structure of observed variables identified by EFA (Hair et al., 2019). In this analysis, the model fit indices are considered to assess how well the model fits the data. According to Table 5, the relative Chi-Square value is found to be 4.021, which is below the recommended threshold of 5.0 (March & Hocevar, 1985). The Comparative Fit Index (CFI) stands at 0.855, matching the recommended threshold (Bentler, 1990). The Root Mean Residual (RMR) is 0.061, below the suggested threshold of 0.08 (Hu and Bentler, 1998). The Goodness of Fit Index (GFI) is calculated at 0.887, which aligns with the suggested value of 0.90 (Joreskog and Sorbom, 1993). The Adjusted Goodness of Fit Index (AGFI) matches the recommended threshold at 0.882 (Anderson and Gerbing, 1984). Furthermore, the Root Means Square Error of Approximation (RMSEA) is 0.074, which is less than the suggested fit (Cudeck & Browne, 1992). Lastly, the Standardized Root Mean Square Residual (SRMR) is 0.071, also falling below the recommended threshold (Cudeck & Browne, 1992). Overall, the indices indicate an acceptable fit of the model to the data, providing validation for the constructs measured by the questionnaire.

Table 5: Confirmatory factor analysis

Model fitting index	*Value*	*Level of acceptance*
Chi-square/df	4.021	<5.0
Comparative fit index (CFI)	0.855	>0.90
Root mean residual (RMR)	0.061	<0.08
Goodness of fit index (GFI)	0.887	>0.90
Adjusted goodness of fit index (AGFI)	0.833	>0.85
Root means square error of approximation (RMSEA)	0.074	<0.08
Standardized root mean square residual (SRMR)	0.071	<0.08

7. CONCLUSIONS, IMPLICATIONS AND LIMITATIONS

In the dynamic and ever-evolving realm of blockchain and smart contract technology, organizations are required to maintain a high degree of agility and adaptability to capitalize on emerging trends. The framework for enhancing internal controls in smart contracts on the blockchain is designed to accommodate these changes and position organizations at the forefront of innovation. Several key future trends, including interoperability, decentralized finance (DeFi), tokenization, privacy enhancements, scalability solutions, smart contract auditing, regulatory compliance, artificial intelligence and blockchain integration, environmental concerns, and quantum-safe cryptography, are significantly influencing the blockchain landscape (Assiri & Humayun, 2023).

This framework seamlessly integrates with these trends, providing organizations with the flexibility to adapt and thrive in this rapidly changing landscape. By embracing this adaptable framework, organizations can effectively navigate the challenges posed by blockchain and smart contract technology. It not only mitigates risks and enhances security but also fosters trust, streamlines operations, ensures compliance, and adjusts to the continually evolving blockchain landscape. This proactive approach positions organizations to fully capitalize on the potential of blockchain technology while effectively managing associated risks, ensuring that they are well-prepared to embrace the future of blockchain and smart contracts. In the ever-changing world of blockchain technology, ensuring strong internal controls for smart contracts is crucial. Our comprehensive framework provides a structured and invaluable approach to meet this imperative, offering significant and far-reaching benefits. Firstly, it builds trust and security by prioritizing integrity, ethical values, and organizational competence. This fosters transparency and honesty, engendering trust among stakeholders. Furthermore, it enforces accountability, reducing the risk of fraudulent activities and enhancing overall security. Secondly, the framework significantly improves risk management by emphasizing the importance of setting objectives and assessing risks. It provides organizations with a clear roadmap to identify and mitigate potential threats. Through tailored control activities, the framework enables proactive risk management, reducing the likelihood of costly errors or security breaches. Thirdly, integrating control activities into daily operations through well-documented policies and procedures strengthens control effectiveness and streamlines organizational processes. This leads to improved operational efficiency, reduced costs, and enhanced adaptability to changes in the blockchain landscape. Furthermore, the framework prioritizes transparency and compliance through regular evaluations and audits to ensure processes adhere to established controls and standards.

The proposed comprehensive framework also addresses data security and privacy controls, safeguarding data integrity and confidentiality, and ensuring compliance with data protection regulations. Lastly, as the blockchain landscape evolves, so do the associated risks and opportunities. This adaptable, comprehensive framework empowers organizations to effectively incorporate emerging technologies and blockchain consensus mechanisms, ensuring ongoing integrity, security, and reliability in the face of rapid innovation.

This study has limitations regarding the continuous need to accommodate the framework to rapid regulation changes, emerging blockchain innovations, and evolving cybersecurity threats. To overcome this limitation, future work can continuously update and dynamically adapt to rapid changes. This will require a structured process to regularly review and update the framework components, ensuring alignment with the evolving regulatory environment and emerging technological advancements in blockchain. Additionally, future research using other frameworks, such as ISO 27001 or internal controls over financial reporting (ICFR), is recommended.

Acknowledgment

The authors would like to express their sincere gratitude to Dr. Mohamed Gomaa, California State Polytechnic University, Department of Accounting, California, Pomona, USA, for his invaluable guidance, mentorship, and support throughout the research and writing process of this article.

Conflict of Interest

There is no conflict of interest involved in the publication of this paper.

References

Anderson, J., & Gerbing, D. (1984). The effect of sampling error on convergence, improper solutions, and goodness-of-fit indices for maximum likelihood confirmatory factor analysis. *Psychometrika,* 49(2), pp.155–173.

Assiri, M., & Humayun, M. (2023). A blockchain-enabled framework for improving the software audit process. *Applied Sciences*, 13(6), pp. 3437.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. *International Conference on Principles of Security and Trust*, 7(2), pp.164-186.

Bari, M.W., Fanchen, M. & Baloch, M.A. (2016). TQM soft practices and job satisfaction; Mediating role of relational psychological contract. *Procedia-Social and Behavioral Sciences,* 235, pp. 453-462.

Bayón, P. S. (2019). Key legal issues surrounding smart contract applications. *SSRN Electronic Journal*, 9(1), pp. 63-91.

Bentler, P. (1990). Comparative fit indexes in structural models. *Psychol. Bull.* 107(2), pp.238–246.

Brender, N., Gauthier, M., Morin, J.-H. & Salihi, A. (2023). Three lines model paradigm shift: a blockchain-based control framework, *Journal of Applied Accounting Research*, 25(1), pp. 149-170.

Cudeck, R. & Browne, M.W. (1992). Alternative ways of assessing model fit. *Sociological Methods and Research,* 21 (2), pp. 230-258.

Budayan, C. & Okudan, O. (2023). Assessment of barriers to the implementation of smart contracts in construction projects evidence from Turkey. *Buildings*, 13(8), 2084.

Casey, M. J., & Vigna, P. (2018). *The Truth Machine: The Blockchain and the Future of Everything*. St. Martin's Press.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise risk management: Integrating with strategy and performance*. Retrieved from https://www.coso.org/Documents/2017-COSO-ERMIntegrating-with-Strategy-and-Performance-Executive-Summary.pdf.

Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials,* 20(4), pp. 3416-3452.

Crenshaw, A. (2021). Statement on DeFi Risks, Regulations, and Opportunities. *U.S. Securities and Exchange Commission (SEC*). Retrieved from https://www.sec.gov/news/statement/crenshaw-defi-20211109**.**

Doekhi, R.J.M. (2023). *The Intercompany Settlement Blockchain: Benefits, Risks, and Internal IT-Controls.* In: Berghout, E., Fijneman, R., Hendriks, L., de Boer, M., Butijn, BJ. (eds) Advanced Digital Auditing. Progress in IS. Springer, Cham.

Ellul, J., Galea, J., Ganado, M., Mccarthy, S. & Pace, G. (2020). Regulating blockchain, DLT and smart contracts: a technology regulator's perspective. *ERA Forum*, 21, pp. 209–220.

Ettish, A. A., El-Gazzar, S. M., & Jacob, R. A. (2017). Integrating internal control frameworks for effective corporate information technology governance. *JISTEM-Journal of Information Systems and Technology Management,* 14(3), pp. 361-370.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate Data Analysis* (8th ed.). Cengage Learning.

Hasan, M.R., Alazab, A., Joy, S.B., Uddin, M.N., Uddin, M.A., Khraisat, A., Gondal, I., Urmi, W.F., & Talukder, M.A. (2023). Smart Contract-Based Access Control Framework for Internet of Things Devices. *Computers,* 12 (11), pp. 240.

Hosain, M., Ameen, M., Mustafi, A., & Parvin, T. (2021). Factors affecting the employability of private university graduates: an exploratory study on Bangladeshi employers. *PSU Research Review,* 7(3), pp. 163- 183.

Hu, L. & Bentler, P. (1998) Fit indices in covariance structure modeling: sensitivity to underparame-terized model misspecification. Psychol. Methods, 3(4), pp. 424–453.

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, 95(1), pp. 118-127.

ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. Retrieved from https://www.isaca.org/resources/cobit/cobit-5.

Joreskog, K. & Sorbom, D. (1993). LISREL 8: Users' Reference Guide. Scientific Software International, IL (1993).

Kalyani, V. & Murugan, K.R. (2021). Implementation of internal control over financial reporting (ICFR) framework and CSR activity- a case study of public company in India. *An international bilingual peer-reviewed research journal*, 11, (01), pp. 111-117.

Kamil, Y., Lund, S. & Islam, M.S. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden. *Inf Syst E-Bus Manage* 21, pp.699–722.

Kannan, V. & Tan, K. (2015). Just in time, total quality management, and supply chainmanagement: understanding their linkages and impact on business performance. *Omega* 33(2), pp.153–162.

Khan, S.N., Loukil, F., Ghedira-Guegan, C. Benkhelifa, E., and Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Netw. Appl. 14, pp. 2901–2925.

Kim, C. Y., & Lee, K. (2018). Risk Management to Cryptocurrency Exchange and Investors: Guidelines to Prevent Potential Threats. *International Conference on Platform Technology and Service ((*PlatCon), South Korea.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)*, pp. 839–858.

Lee, H., & Wie, D. (2023). Gone with the fire: Market reaction to cryptocurrency exchange shutdown. *Heliyon*, 9(7), e18231.

Lu, Q., Xu, X., Liu, Y., & Zhang, W. (2018). Design Pattern as a Service for Blockchain Applications, *International Conference on Data Mining Workshops (ICDMW).*

Marko, R., & Kostal, K. (2022). Management of Decentralized Autonomous Organizations. *IEEE International Conference on Omni-layer Intelligent Systems (COINS),* Spain.

Morrison, R., Mazey, N. C. H. L., & Wingreen, S. C. (2020). The DAO Controversy: The Case for a New Species of Corporate Governance. *Front Blockchain, Sec. Smart Contracts*, 3. Retrieved from: Frontiers | The DAO Controversy: The Case for a New Species of Corporate Governance? (frontiersin.org).

Nachrowi, E., Nurhadryani, Y., & Sukoco, H. (2020). Evaluation of governance and management of information technology services using Cobit 2019 and ITIL 4. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi),* 4(4), pp.764-774.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

National Institute of Standards and Technology (NIST) (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)

Popper, N. (2016). *The Inside Story of the DAO Hack. The New York Times*.

Queiroz, M. M., Wamba, S. F., Bourmont, M. D., & Telles, R. (2020). Blockchain adoption in operations and supply chain management: Empirical evidence from an emerging economy. *International Journal of Production Research*, 59(6), pp.1-17.

Rozario, M.A., & Thomas, C. (2019). Reengineering the audit with blockchain and smart contracts. *Journal of Emerging Technologies in Accounting*. 16 (1), pp. 21–35.

Sheldon, M. D. (2019). A primer for information technology general control considerations on a private and permissioned blockchain audit. *Current Issues in Auditing*, 13(1), pp. A15-A29.

Singh, A., Parizi, R. M., Qi, Z., Choo, K. R., & Dehghantanha, A. (2019). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Computers & Security*, 88, pp. 101654.

Sreejith, R., & Senthil, S. (2023). Smart Contract Authentication assisted Graph Map-Based HL7 FHIR architecture for interoperable e-healthcare system. *Heliyon*, 9(4), pp. e15180.

Taherdoost, H. (2023). Smart contracts in blockchain technology: A critical review. *Information*,14 (2), pp. 117.

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. *Penguin*. Retrieved from https://www.amazon.com/Blockchain-Revolution-Technology.

Vincent, N., & Barkhi, R. (2021). Evaluating blockchain using COSO. *Current Issues in Auditing,* 15(1), pp. A57–A71.

Xu, Y., Chong, H., & Chi, M. (2021). A review of smart contracts applications in various industries: A procurement perspective. *Advances in Civil Engineering.* Retrieved from: A Review of Smart Contracts Applications in Various Industries: A Procurement Perspective (wiley.com).

Zhang, F., Cecchetti, E. Croman, K., & Shi, E. (2016). Town Crier: An Authenticated Data Feed for Smart Contracts. *Conference on Computer and Communications Security*, pp. 270-282.

Zheng, S., Hu, Y., Chong, A. Y. L., & Tan, C-W. (2022). Leveraging blockchain technology to control contextualized business risks: Evidence from China. *Information & Management*, 59(7), pp.103628.

Appendix 1

Framework Component	*Principles and Control Activities*	*Relevant Frameworks*	*Guidelines*
Control Environment	Demonstrate commitment to integrity and ethical values	COSO	Establish a strong ethical foundation within the organization, showcasing unwavering commitment to integrity and ethical values at all levels
	Exercise oversight responsibility by the board of directors		The board of directors plays a crucial role in exercising oversight responsibility. They provide governance and ensure that the organization operates ethically and in line with its mission. This oversight involves reviewing and approving strategic plans, assessing risks, and monitoring management's activities
	Establish structures, reporting lines, and appropriate authorities and responsibilities		Effective internal control requires well-defined structures and reporting lines. Roles, responsibilities, and authorities should be clearly delineated. This ensures accountability and prevents conflicts of interest. Well-structured reporting lines facilitate timely communication and decision-making.
	Demonstrate commitment to competence		Organizations should prioritize the competence of their personnel. This involves recruiting, developing, and retaining skilled individuals who can execute their responsibilities effectively. Competence enhances the organization's ability to achieve its objectives while minimizing the risk of errors.
	Enforce accountability for internal control		Accountability ensures that individuals are responsible for their actions related to internal controls. When there's accountability, employees are more likely to adhere to control procedures, fostering a robust control environment.
Risk Assessment and Management	Specify suitable objectives	COBIT	Clear objectives must be established to guide risk assessment efforts. These objectives should align with the organization's mission and strategic goals, providing a context for risk evaluation.
	Identify and assess risks.	COSO	Organizations need to identify potential risks that could hinder the achievement of objectives. This involves assessing the likelihood and impact of risks to prioritize them for further analysis

Design and Development	Involve internal control experts during smart contract design	COSO	Implement secure coding practices. Conduct code reviews and vulnerability assessments.
	Leverage NIST guidelines for secure software development	NIST	Follow NIST for blockchain security. Implement secure coding practices and cryptographic controls
Testing and Deployment	Perform thorough testing of smart contracts	NIST	Unit testing, integration testing, and security testing. private networks for initial deployment. Monitor deployment for any unexpected behavior.
Monitoring and Continuous Improvement	Perform ongoing and/or separate evaluations.	COSO	Regular assessments are necessary to verify the presence and effectiveness of internal control components. The COSO framework underscores the need for ongoing and separate evaluations to ensure the control environment remains robust.
	Evaluate and communicate deficiencies.		Identifying deficiencies in internal controls is essential for addressing vulnerabilities. The Monitoring and Continuous Improvement principle in the COSO framework emphasizes evaluating and communicating internal control deficiencies to relevant parties.
Security and Compliance	Address security aspects	ITIL	Encryption, access controls, identity management, implement security measures to protect data.
	Comply with relevant regulations		Stay informed about legal and regulatory requirements (e.g., GDPR, AML). Ensure compliance with privacy regulations.
	Document control procedures and maintain an audit trail.		Once control activities are defined, they need to be integrated into the organization's operations through well-documented policies and procedures. This ensures that control measures are consistently implemented.
Collaboration and Transparency	Collaborate with other entities in the blockchain network	COSO	Ensure transparency in smart contract execution. Consider multi-signature controls for critical transactions.