Journal of Engineering and Technology for Industrial Applications

ISSN ONLINE: 2447-0228

ITEGAM-JETIA

Manaus, v.11 n.54, p. 172-180. July/August., 2025.

DOI: https://doi.org/10.5935/jetia. v11i54.1710

RESEARCH ARTICLE OPEN ACCESS

RISK MANAGEMENT AND GOVERNANCE IN BLOCKCHAIN-BASED DIGITAL IDENTITY PROJECTS: A BUSINESS ANALYSIS AND PROJECT MANAGEMENT FRAMEWORK

Tobiloba Kazeem[1], Olatoye Kabiru Agboola[2], Nonso Okika[3], Soyingbe FolasadeOwoolaAdebayo[4] Fope Opeola[5], Nnenna Linda Akunna[6], Oreoluwa Serifat Abimbola[7]

[1]Western Illinois University: Macomb, Illinois, US.
[2]New Jersey City Universit, US.
[3]University of Michigan, US
[4]Lagos State University, Nigéria
[5]Ntional Oceanography Center, Reino Unido
[6]University of West England, Reino Unido
[7]Nexford University, US

[1]https://orcid.org/0009-0002-2265-0605, [2]http://orcid.org/0009-0004-0905-0175, [3]https://orcid.org/0000-0001-9386-4577
[4]https://orcid.org/0009-0001-6227-5726, [5]https://orcid.org/0009-0004-6245-0522, [6]https://orcid.org/0009-0001-8887-5519
[7]http://orcid.org/0009-0006-5345-7356

Email: tobikazeem4@gmail.com, olatoye.agboola88@hotmail.com, nonnykins23@yahoo.com, shadeowoola@gmail.com, fope.opeola@gmail.com, achoakunna@gmail.com, bimbolady09@yahoo.com

ARTICLE INFO

Article History
Received: March 14, 2025
Revised: April 20, 2025
Accepted: June 15, 2025
Published: August 31, 2025

Keywords:
Blockchain,
Digital Identity,
Risk Management,
Governance,
Project Management.

ABSTRACT

Blockchain is viewed as a revolutionary solution to digital identity management, offering decentralization, security, and user control over one's own private identity. However, there are a number of challenges which hamper its adoption—related to risk management and governance. This study carefully evaluates the integration of the strategies and governance frameworks for avoiding risks in blockchain based digital identity projects. Security vulnerability, regulatory uncertainty and interoperability issues are the key risk to be managed by robust risk management framework such as ISO 31000 and NIST. Governance models, including on-chain and off-chain approaches, influence stakeholder coordination, transparency, and compliance.

While on-chain governance ensures decentralized decision-making through smart contracts, off-chain governance incorporates informal discussions and regulatory oversight. A hybrid governance model is proposed to sustainably and securely implement given that the best of both world can be achieved. From a business analysis and project management standpoint, integrating risk and governance mechanisms is useful because it improves decision making, coordination of stakeholders, as well as regulatory alignment. Based on the findings of this study, it serves as a strategic insight that organizations, project managers and policymakers should consider when working in blockchain identity ecosystems.

I. INTRODUCTION

Blockchain technology has transformed digital identity management by offering decentralized, verifiable, and tamper-resistant identity solutions [1]. Blockchain based digital identity differs from the traditional identity systems where databases are centralized and involve the least security and transparency of user data [2]. The growing adoption of blockchain in identity management is driven by concerns over data breaches, identity theft, and inefficiencies in conventional identity verification processes [3].

Despite its advantages, blockchain-based digital identity havecomplex challenges that call for strong governance and risk management structures. Key risks are security threats including cryptographic attack, by smart contract vulnerability, and smart contract

vulnerabilities [1]. Furthermore, data protection, compliance and verification of cross border identity is highly implementation challenged [2]. This exacerbates the lack of standardized governing frameworks in implementing blockchain since it results in fragmentation and can lead to interoperability problems across various blockchain networks [4]. According to Tan et al. (2022) [5], governance is fundamental to assuring the alignment of blockchain based digital identity projects to the legal and ethical considerations. Unlike traditional centralized identity management, blockchain governance requires coordination among multiple stakeholders including developers, regulators, businesses and end users in deciding the decision making and policy enforcement [6].

Role, responsibility and accountability mechanisms are defined for effective governance of structures, to prevent misuse, complying with data protection laws and for dispute resolution [5]. From the business analysis and project management perspective, it is required to integrate a risk management and governance frameworks in blockchain based digital identity projects to their success. Technical, regulatory and operational risks must be assessed by business analysts and project managers, they must align with stakeholders and strategic objectives [6]. This necessitates an interdisciplinary approach that combines risk assessment methodologies, compliance strategies, and governance models tailored to blockchain technology. By addressing these complexities, organizations can leverage blockchain-based digital identity solutions to enhance security, privacy, and operational efficiency while mitigating associated risks [6].

Therefore, this study aims to investigate risk management strategies and governance frameworks in blockchain-based digital identity projects, focusing on their integration into business analysis and project management to enhance security, compliance, and stakeholder coordination.

RESEARCH AIM AND OBJECTIVES

The primary aim of this study is to investigate risk management strategies and governance frameworks in blockchain-based digital identity projects, focusing on their integration into business analysis and project management to enhance security, compliance, and stakeholder coordination. This research evaluates the effectiveness of existing governance models and risk mitigation approaches, providing insights into their practical application in decentralized identity systems.

The key objectives of this study are:

1. To review existing literature on risk management strategies in blockchain-based digital identity projects and assess their effectiveness.
2. To examine governance models that facilitate stakeholder coordination, regulatory compliance, and sustainable implementation in decentralized identity systems.
3. To identify key challenges in integrating risk management and governance into blockchain-based digital identity projects, including security risks, regulatory uncertainties, and interoperability issues.
4. To propose strategic business and project management recommendations for organizations seeking to implement secure and well-governed blockchain-based digital identity solutions.

This study provides valuable insight into the critical risk and governance issues in blockchain based digital identity projects to the field of Business Analysis and Project Management. With the rise in blockchain adoption, organizations have come to realize that they must come up with a viable strategy in addressing the risks entailed while meeting the demands of the varied regulatory frameworks. This research fills the knowledge gap by structuring the way by which risk management and governance can be integrated into blockchain based identity initiatives.

The findings from a business perspective provides organizations with insights to better develop decision making process, set up better risk assessments and have the means to establish governance mechanisms. This also provides an outlook to policymakers and regulators on how to perform the balancing security, privacy, and compliance when creating decentralized identity system. Additionally, the results of this research are important for project managers and business analysts engaged in blockchain implementations. The study provides practical recommendations and case study insights as the tools to establish and manage blockchain digital identity projects.

II. LITERATURE SEARCH STRATEGY

A systematic approach was employed to identify relevant literature on risk management and governance in blockchain-based digital identity projects. The search strategy involved querying academic databases such as Scopus, Web of Science, IEEE Xplore, and Google Scholar, as well as industry reports and regulatory guidelines. Keywords included “blockchain governance,” “risk management in blockchain,” “digital identity security,” “decentralized identity frameworks,” and “blockchain compliance.” Boolean operators (AND, OR) were used to refine search results and ensure the inclusion of interdisciplinary perspectives.

Only those peer reviewed journal articles published between 2019 to 2024 were considered for the review to make the review more robust. This timeframe was determined as it enables capturing the latest blockchain identity governance, regulatory trends and risk management frameworks. It was also performed backward and forward citation tracking to identify influential studies. The studies were categorized thematically, namely, a review of risk mitigation strategies, governance models and project management implications. The search strategy integrated literature from business analysis, project management, cybersecurity and legal perspectives, that together with other sources of literature ensure the thorough examination of the blockchain based digital identity challenges and best practices.

Inclusion and Exclusion Criteria

To maintain research validity and relevance, specific inclusion and exclusion criteria were applied during the literature selection process.

Inclusion criteria:

1. Studies focusing on risk management and governance in blockchain-based digital identity systems.
2. Peer-reviewed journal research published between 2019 and 2025 to ensure up-to-date insights.

3. Literature addressing the intersection of blockchain, digital identity, business analysis, and project management.
4. Empirical studies and theoretical frameworks that provide strategic insights into blockchain governance and risk management.

Exclusion criteria:

1. Articles unrelated to blockchain-based digital identity or those discussing general blockchain applications without governance or risk management perspectives.
2. Non-peer-reviewed sources such as blogs, opinion pieces, and non-academic reports lacking empirical or theoretical rigor.
3. Studies published before 2019 unless they provide foundational theoretical concepts.
4. Research focusing solely on technical aspects without business, governance, or risk considerations.

Analysis Framework

The literature was analyzed using a thematic synthesis framework to identify key patterns, relationships, and gaps in risk management and governance for blockchain-based digital identity projects. Thematic analysis was chosen for its ability to integrate multidisciplinary perspectives and extract meaningful insights from diverse sources.

The analysis was structured into three key themes:

1. **Risk Management Strategies:** This theme looked at studies related to security threats, regulatory risks, and operational challenges to blockchain identity project [7]. Through risk mitigation frameworks, it found such safety measures as cryptographic security, compliance protocols and resilience strategies.
2. **Governance Models:** This section explored decentralized governance structure, stakeholder coordination mechanism and regulatory compliance approaches [8]. Therefore, it analyzed governance models of achieving the necessary balance between autonomy and regulation of digital identity systems.
3. **Integration into Business Analysis and Project Management:** This theme investigated incorporation of the risk management and governance frameworks into the project lifecycle planning, stakeholder management, and compliance strategies [9].

III. THEORETICAL BACKGROUND

III.I BLOCKCHAIN-BASED DIGITAL IDENTITY SYSTEMS

Digital identity is the set of attributes that defines an individual in the digital space and that supports authenticating and verifying an individual in the online interactions [10]. Centralized databases used by the traditional identity management systems are highly vulnerable to security breaches, unauthorized access and possible privacy violations [11]. Hence. the blockchain technology provides a decentralized viable option where people, guided by self-sovereign identity (SSI) can no longer rely on central authorities and hence are less exposed to the risks of having a single point of failure [10], similarly, Blockchain technology introduces an innovative approach by establishing a decentralized, transparent, and cryptographically secure platform for identity verification and data exchange [12]. In addition, the immutability of blockchain adds to the data integrity as identity records cannot be altered or deleted [13].

Furthermore, cryptographic security mechanisms such as encryption and zero-knowledge proofs ensure privacy of users as well as provide a secure and verifiable way of user identity authentication [14]. However, blockchain based digital identity systems have limited challenges. Still, the primary concern is scalability as high transaction costs and slow processing speed in public blockchains can keep public blockchains on a small scale of adoption [10]. Moreover, interoperability barriers make it difficult to interoperate BlockChain based identity solution with existing digital identity framework for cross platform usage [13].

As GDPR will continue to constrain adoption, regulatory uncertainty also exacerbates adoption challenges in jurisdictions that require strict data protection such as the General Data Protection Regulation. There is the issue of compliance and the protection of privacy because the immutable nature of blockchain is a fundamental contradiction to legal requirements like the right to erasure [11]. In addressing these challenges, such robust risk management and governance framework is needed, that secures the security, adhere to the regulatory requirements, and interoperable. Decentralization and oversight mechanism should be balanced to provide a secure and scalable and legally compliant blockchain based digital identity systems [14]. Blockchain identity solutions can create enough integration of strategic risk mitigation measures, regulatory frameworks to ensure scalability and to maintain security and trust in digital interactions.

RISK MANAGEMENT IN BLOCKCHAIN PROJECTS

Risk management is a fundamental aspect of blockchain-based digital identity projects, as these systems face significant security, scalability, and compliance challenges. Established frameworks such as ISO 31000, NIST, and COBIT provide structured methodologies for identifying and mitigating risks [15]. However, blockchain's decentralized nature introduces unique vulnerabilities that require tailored risk management approaches. Security risks remain a primary concern, with smart contract vulnerabilities potentially leading to identity fraud and unauthorized access [16]. Additionally, Cryptographic key management can be viewed from two categories: Secret keys [17] and public/private key [18]. Private key mismanagement can result in permanent identity loss, while inadequate encryption mechanisms increase the likelihood of data breaches [19]. Scalability issues further hinder the adoption of blockchain-based identity solutions, as high transaction fees and network congestion create inefficiencies [20]. Compliance risks also pose challenges, particularly regarding regulatory conflicts such as GDPR's right to data modification, which contrasts with blockchain's immutability [15].

A comprehensive risk management framework that integrates cybersecurity, governance, and compliance measures is essential for the successful implementation of blockchain-based digital identity projects [21]. Governance in blockchain projects is crucial for ensuring transparency, stakeholder participation, and regulatory compliance. It defines the decision-making structures that influence how digital identity systems evolve, resolve disputes, and maintain security [22]. Given the decentralized nature of blockchain, governance frameworks must carefully balance autonomy, accountability, and coordination while addressing regulatory concerns [23]. Effective governance mechanisms are essential to preventing centralization risks, ensuring equitable decision-making, and fostering long-term sustainability in blockchain-based digital identity [21]

GOVERNANCE IN BLOCKCHAIN PROJECTS

One of the popular governance models is on chain governance, which function through smart contracts and token-based voting [23]. As this protocol is a decentralized one, the change to the protocol can be automated and completed by a set of stakeholder votes, or through DAOs [24]. Although this increases transparency and efficiency, the concentration of the ownership of the tokens also brings the risk of governance centralization [25].

On the other hand, off chain governance is through informal methods such as developer discussion, regulatory negotiation and community led decision making. It also involves providing deep and valuable enhancements. Nevertheless, this method can result in lack of transparency and over representation of key stakeholders [26]. Governance over blockchain, have challenges including transparency, centralization risks and regulatory uncertainty. To resolve these challenges, the hybrid form of governance which comprises of both on chain and off chain elements can coincide the balance between decentralization, flexibility and regulatory compliance [24]. When blockchain based digital identity projects integrate automation with structured decision-making process, it can help in improving the efficiency of governance while maintaining trust and security [23].

IV. RESULTS AND DISCUSSIONS

This thematic analysis critically examines existing literature, categorizing the discussion into three core themes: risk management strategies, governance models, and the challenges of integrating risk management with governance in blockchain-based digital identity systems.

RISK MANAGEMENT STRATEGIES IN BLOCKCHAIN-BASED DIGITAL IDENTITY PROJECTS

A central theme in the literature is the effectiveness of risk management strategies in blockchain-based digital identity systems. As Zyskind & Nathan (2015) [27] stated, the main advantage of blockchain's decentralization is to significantly reduce data breaches and single points of failure, which has been a thorn in the side of centralized identity management for many years. Likewise, Wüst and Gervais (2018) [28] claim that blockchain serves to increase data integrity and authentication via cryptographic mechani, sms of verification, thus preventing identity records from being tampered with. However, Atzei et al. (2016) [29] emphasize blockchain's weaknesses, especially the smart contract risks. According to them, the 2016 DAO hack in which attackers stole $50 million from a smart contract due to a reentrant bug is an example of how coding flaws in smart contracts can be exploited.

According to Zhou et al. (2022) [30], this argument is supported since, once deployed, self-executing contracts cannot be changed and errors and vulnerabilities are more damaging. Besides security concerns, scalability turns out to be another major risk. Nguyen et al. (2021) [31] feel that, while proof of work (PoW) consensus mechanisms are secure, they are also inefficient and so large-scale identity verification is not possible. According to [32] proof of stake (PoS) mechanisms are an alternative to PoW that should solve scalability problems in an energy efficient manner. Yet, [33] contradicts this optimism by arguing that PoS brings in new risks, including economic centralization whereby the wealthy take control of network governance. This also involves a trade-off between security and efficiency that is characteristic of lack of a standardized risk management framework for blockchain identity projects. Even though there are those who suggest that the already existing frameworks, ISO 31000 and NIST risk management guidelines, can be applied to blockchain identity projects, [34] states that the root problem lies in these frameworks do not consider blockchain's unique risks like 51% attacks and vulnerabilities of a decentralized governance. Hence [35] suggest customized risk assessment models that take into consideration risk inherent to blockchain's operating.

GOVERNANCE MODELS FOR STAKEHOLDER COORDINATION, REGULATORY COMPLIANCE, AND SUSTAINABILITY

Another key theme in the literature is governance, which is crucial for coordinating the stakeholders, complying with the regulations and for the long-term sustainability of the blockchain based digital identity projects. According to [36], blockchain's strong point is in decentralizing decision-making power to users rather than central authorities. Following this sentiment, [37] describes on chain governance models, which are executed through Decentralized Autonomous Organizations (DAOs) as allowing for more transparent, and in some sense more democratic decisions. However, [38] present a more diverse view, acknowledging that while DAOs promote decentralization, they also introduce governance inefficiencies, particularly in dispute resolution and protocol upgrades.

Wang and De Filippi (2020) [39] extend this discussion to self-sovereign identity (SSI) models, which empower users to control their identity data without relying on intermediaries. They argue that SSI is in line with the blockchain's principles of user autonomy and privacy preserving. Interestingly, however, [8] counter this by arguing that there are more legal and regulatory barriers to clear decentralized identity systems. Specifically, they point to conflict between blockchain immutability and the General Data Protection Regulation (GDPR) in relation to the "right to be forgotten." Where [40] agrees the problem of GDPR compliance is especially difficult for blockchain identity solutions, the brief note that technological 'workarounds' such as zero knowledge proofs (ZKPs) could enable the selective erasure of data without compromising the integrity of the blockchain. However, some scholars call for the decentralization but believe that fully decentralized governance models are impossible to realize.

According to [32], many blockchain networks, and especially Ethereum, have not achieved much in the way of decentralisation because core developers and influential stakeholders retain their control. This argument is reinforced by [34] who point out that in reality, early adopters and wealthier participants tend to consolidate power in such a manner that there is a kind of spontaneous centralization. In order to handle these issues, some researchers suggest hybrid forms of governance. Hyperledger Indy is one such example of a permissioned blockchain where transactions are still based on decentralised principles, but are validated by trusted entities, as mentioned by [41]. According to them, such models find the right balance between decentralization and regulatory oversight, which means that they

will be more compliant with legal frameworks. However, critics like [42] point out that by reintroducing aspects of centralization, hybrid models simply reintroduce trustless aspects that are inherent to many blockchain based solutions for identity.

CHALLENGES IN INTEGRATING RISK MANAGEMENT AND GOVERNANCE IN BLOCKCHAIN-BASED DIGITAL IDENTITY PROJECTS

Blockchain based digital identity projects face a multifaceted challenge where it is difficult to establish how risk management and governance should be integrated. Concerning security risk, [39] states that blockchain does not prevent users from having a centralized database, but instead puts the full responsibility on the user for protecting his credentials. They argue that this makes private keys lost or compromised more likely to result in permanent identity loss. Yaacoub et al. (2023) [43] also discuss the implication of recovery mechanisms for security of blockchain based identity systems, noting that if such systems have backdoors for recovery, then they will undermine the very security principles they seek to uphold.

Apart from the security concerns, [8] also pointed out regulatory uncertainty as the main obstacle to the adoption of blockchain identity. However, governments across the world remain skeptical about decentralized identity solutions as they are concerned about their potential to be used in fraud and money laundering. For example, China has been very strict with the development of the decentralized identity, while the European Commission's eIDAS 2.0 proposal aims at including blockchain based identity in formal and legal frameworks [44]. As long as it represents progress towards regulatory acceptance, [8] assert that legal ambiguity remains and continues to discourage widespread implementation and investment. Interoperability is another persistent challenge.

According to [45], most blockchain based identity projects operate in a siloed environment where it is difficult to verify a cross-platform identity. Furthermore, it mentions the work going on by the World Wide Web Consortium (W3C) to make Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to become the standard in standardizing blockchain identity protocols. Rikken et al. (2019) [46] concede that these efforts have, however, not resolved the fragmentation problem as various blockchain networks have different governance models and security standards. There are emerging technological solutions, which may provide pathways to solution. George and Kizhakkethottam (2021) [47] proposes homomorphic encryption and zero knowledge proofs as promising ways to improve privacy while maintaining compliance with the data regulations. Meanwhile, [48] explains that cross chain identity verification protocols are means to enable interoperability among the blockchain ecosystems. While these advancements hold promise, their real-world adoption remains limited, and further research is needed to refine their implementation within blockchain identity frameworks.

V. IMPLICATIONS FOR BUSINESS ANALYSIS AND PROJECT MANAGEMENT

BUSINESS ANALYSIS INSIGHTS

A bridging of technical, regulatory, and business considerations is essential for the success of blockchain based digital identity projects and business analysts fill this role very well. First it is important to understand risk management in whole and to identify vulnerabilities with respect to smart contracts, cryptographic key management and scalability limits.

Business analysts play a crucial role in leveraging smart contracts to automate compliance and governance processes. Traditional systems rely on manual tasks such as document verification, reporting, and auditing to ensure regulatory compliance. These processes are not only time-consuming but also susceptible to human error [49]. By integrating smart contracts, business analysts help organizations streamline compliance by automating checks and governance tasks [50]. Smart contracts can be designed to enforce regulatory compliance in real-time by monitoring transactions and verifying adherence to key regulations, such as Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements [51].

Business analysts are responsible for defining the regulatory parameters and business rules that smart contracts must follow. They ensure that these contracts are programmed to halt transactions if compliance conditions are not met, thereby preventing violations and mitigating financial an legal risks. By translating complex regulatory requirements into actionable smart contract functionalities, business analysts enhance operational efficiency, reduce compliance costs, and minimize risks associated with non-compliance.

Additionally, Business analysts play a critical role in understanding and managing risks associated with cryptographic key management. By identifying vulnerabilities and designing effective mitigation strategies, they help ensure that an organization's data remains secure. Cryptographic key management can be viewed from two categories and the associated risks: Secret keys and public/private key [52].

Secret keys are used for both encryption and decryption with symmetric cryptographic algorithms, as well as for ensuring data integrity through mechanisms like message authentication codes (e.g., HMAC) [52]. Since the same key is employed for encryption and decryption, any compromise of this key can lead to significant security breaches. Business analysts must assess risks such as unauthorized access, key leakage, and the overall lifecycle management of these keys, recommending stringent access controls and regular audits to mitigate potential vulnerabilities.

Whereas, public/private key pairs involve two mathematically linked keys used in asymmetric cryptography for authentication, digital signatures, or secure key establishment [46]. The private key, which must remain confidential at all times, is crucial for maintaining the integrity of the system. Meanwhile, the public key is shared to facilitate secure communications. For business analysts, the key risk is ensuring that the private key is adequately protected, as its exposure could allow malicious parties to impersonate legitimate users or compromise the entire cryptographic system [49].

By understanding these two categories and the associated risks, business analysts can develop comprehensive risk management strategies that not only safeguard cryptographic assets but also support overall regulatory compliance and operational efficiency.

Furtermore, Business analysts play a critical role in understanding and managing the risks associated with the scalability limits of blockchain systems. As the number of stakeholders increases and the volume of shared data grows—often beyond traditional logistic data—the blockchain's on-chain data sharing mechanism may face significant scalability challenges (Hariyani et al., 2025) [53]. This can lead to performance bottlenecks and operational inefficiencies that jeopardize the system's overall effectiveness. As more participants

join, the increased load may slow down transaction processing or even cause system delays. Recognizing these vulnerabilities early is essential for developing effective risk management strategies. Business analysts must evaluate how the influx of diverse stakeholders and the resulting massive data exchanges can stress the blockchain infrastructure [54].

Since blockchain is immutable, analysts need to examine regulatory frameworks, such as GDPR to comply in terms of security and privacy. It is worth noting that the stored records have to be secured in order to prevent unauthorized processing, accidental loss, destruction, or damage (integrity and confidentiality principle). However, public blockchains must take some steps to secure data with appropriate measures, such as using encryption or anonymization [55].

For this, Business analysts need to find potential conflicts among data protection laws and blockchain design principles as well as mitigation strategies including zero-knowledge proofs, selective disclosure mechanisms, etc. Not only that but the blockchain identity projects have developers, regulators, enterprises, and end users with their own priorities, so stakeholder alignment is another key responsibility. Business analysts must define the business requirements with a defined precedence list of business requirements balancing security, privacy, and operational efficiency whereas the solution also needs to meet technical feasibility and regulatory mandates. Furthermore, it is important to choose governance model (onchain, offchain, or hybrid) in consistence with the strategic goals of the organization. Business analysts help decision makers by translating complex technical and compliance challenge to structured business insights to guide sustainable and secure blockchain identity implementation to further trust, efficiency and viability in a decentralized identity ecosystem.

PROJECT MANAGEMENT IMPLICATIONS

Risk management, stakeholder coordination, and governance are some of the complex risks that project managers of blockchain based digital identity projects would need to navigate. A proper, structured approach to the mitigation of risk is necessary, and must take into account the integration of security, compliance, and scalability considerations from project initiation to deployment.

Ensuring adherence to best practices in smart contract development, private key management, and consensus mechanisms is critical in preventing security vulnerabilities and operational failures. Stakeholder management is particularly complex due to the diverse interests involved, including technical teams, regulatory bodies, and end-users. In decentralized structures of governance, consensus building can be slow and fragmented, which means that transparent communication as well as facilitation of decision making are indispensable elements for project managers. Furthermore, the interoperability challenges must be planned carefully so that the integration with the existing identity system is seamless and with any other chain is possible. In this context of the changing regulatory environment, project managers should adopt agile methodologies, which enable iteration of project to technological novelties and legal requirements. Implementing hybrid governance models may necessitate a phased deployment approach, ensuring regulatory compliance without undermining decentralization. Ultimately, ability to deliver secure, scalable, compliant solutions within budget and timeline is the key success factor in delivering blockchain based digital identity ecosystem that is trusted, and meet organizational objective.

V. CONCLUSIONS

This study has shown the importance of risk governance and management on projects of blockchain based digital identity. However, Blockchain provides decentralized, secure and immutable identity management solutions while being a security and scalability risk, along with noncompliance to regulatory compliance. Mitigating the vulnerabilities of smart contracts, mismanagement of private keys, and interoperability falls upon the importance of having that such smart framework as ISO 31000 and NIST. On chain and off chain governance are important governance models needed to maintain transparency, participation of stakeholders and compliance. Combining decentralized decision making with regulatory oversight is needed to increase security and sustainability on a long-term use. As organizations seek to embrace blockchain based digital identity projects, regulatory standards for risk management should be taken into consideration to enhance adoption. This includes smart contract security audits, cryptography key protection measures, and ensuring data privacy laws compliance. On-chain and off-chain mechanisms should be merged into the governance framework to ensure transparency, avoid power centralization and to respond to the regulation change. Standards for the governance and interoperability for any system must be established and those standards must be collaboratively developed amongst the policymakers, industry leaders and the technology developers to work. Project managers should adopt agile methodologies to navigate regulatory changes effectively. Lastly, research about scalable blockchain identity solutions can be further on security, efficiency, and the regulatory alignment.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: Tobiloba Kazeem, Olatoye Kabiru Agboola, Nonso Okika, Soyingbe FolasadeOwoolaAdebayo Fope Opeola, Nnenna Linda Akunna, Oreoluwa Serifat Abimbola.
Methodology: Tobiloba Kazeem, Olatoye Kabiru Agboola, Nonso Okika, Soyingbe FolasadeOwoolaAdebayo Fope Opeola, Nnenna Linda Akunna, Oreoluwa Serifat Abimbola.
Investigation: Tobiloba Kazeem, Olatoye Kabiru Agboola, Nonso Okika, Soyingbe FolasadeOwoolaAdebayo Fope Opeola, Nnenna Linda Akunna, Oreoluwa Serifat Abimbola.
Discussion of results: Tobiloba Kazeem, Olatoye Kabiru Agboola, Nonso Okika, Soyingbe FolasadeOwoolaAdebayo Fope Opeola, Nnenna Linda Akunna, Oreoluwa Serifat Abimbola.
Writing – Original Draft: Tobiloba Kazeem, Olatoye Kabiru Agboola, Nonso Okika, Soyingbe FolasadeOwoolaAdebayo Fope Opeola, Nnenna Linda Akunna, Oreoluwa Serifat Abimbola.
Writing – Review and Editing: Tobiloba Kazeem, Olatoye Kabiru Agboola, Nonso Okika, Soyingbe FolasadeOwoolaAdebayo Fope Opeola, Nnenna Linda Akunna, Oreoluwa Serifat Abimbola.
Resources: Author Two. Tobiloba Kazeem, Olatoye Kabiru Agboola, Nonso Okika, Soyingbe FolasadeOwoolaAdebayo Fope Opeola, Nnenna Linda Akunna, Oreoluwa Serifat Abimbola.

Supervision: Tobiloba Kazeem, Olatoye Kabiru Agboola, Nonso Okika, Soyingbe FolasadeOwoolaAdebayo Fope Opeola, Nnenna Linda Akunna, Oreoluwa Serifat Abimbola.
Approval of the final text: Tobiloba Kazeem, Olatoye Kabiru Agboola, Nonso Okika, Soyingbe FolasadeOwoolaAdebayo Fope Opeola, Nnenna Linda Akunna, Oreoluwa Serifat Abimbola.

VIII. REFERENCES

[1] O. Olawoyin, "Blockchain technology in risk management: Strengthening cybersecurity and financial integrity," Int. J. Res. Publ. Rev., vol. 5, pp. 2336–2348, 2024. doi: 10.55248/gengpi.5.1024.2829.

[2] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," Blockchain Res. Appl., vol. 2, no. 2, p. 100014, 2021. doi: 10.1016/j.bcra.2021.100014.

[3] C. S. Sung and J. Y. Park, "Understanding blockchain-based identity management system adoption in the public sector," J. Enterprise Inf. Manage., vol. 34, no. 5, pp. 1481–1505, 2021. doi: 10.1108/JEIM-12-2020-0532.

[4] R. van Pelt, S. Jansen, D. Baars, and S. Overbeek, "Defining blockchain governance: A framework for analysis and comparison," Inf. Syst. Manage., vol. 38, no. 1, pp. 21–41, 2021. doi: 10.1080/10580530.2020.1720046.

[5] E. Tan, S. Mahula, and J. Crompvoets, "Blockchain governance in the public sector: A conceptual framework for public management," Gov. Inf. Q., vol. 39, no. 1, p. 101625, 2022. doi: 10.1016/j.giq.2021.101625.

[6] H. Bai, Z. Li, K. Chen, and X. Li, "Blockchain-based responsibility management framework for smart city building information modeling projects using non-fungible tokens," Buildings, vol. 14, no. 11, p. 3647, 2024. doi: 10.3390/buildings14113647.

[7] T. B. Makhanya, "The implications for risk management in the era of technological advancements," IntechOpen, 2024. doi: 10.5772/intechopen.1003899.

[8] Y. Zhao and J. Qiu, "Decentralized governance in action: A governance framework of digital responsibility in startups," J. Responsible Technol., vol. 21, p. 100107, 2025. doi: 10.1016/j.jrt.2025.100107.

[9] O. Bakare, R. Aziza, N. Uzougbo, and P. Oduro, "A governance and risk management framework for project management in the oil and gas industry," Open Access Res. J. Sci. Technol., vol. 12, pp. 121–130, 2024. doi: 10.53022/oarjst.2024.12.1.0119.

[10] M. S. Prashanth, R. Karnati, M. S. Velpuru, and H. V. Reddy, "Blockchain-based digital identity management system for cybersecurity," in *Proc. 5th Int. Conf. Data Sci., Mach. Learn. Appl.*, vol. 1273, A. Kumar, V. K. Gunjan, S. Senatore, and Y. C. Hu, Eds., Springer, Singapore, 2025. doi: 10.1007/978-981-97-8031-0_30.

[11] A.-C. Careja and N. Tapus, "Digital identity using blockchain technology," Procedia Comput. Sci., vol. 221, pp. 1074–1082, 2023. doi: 10.1016/j.procs.2023.07.232.

[12] Alliy Adewale Bello , David Amoah Oduro , Emmanuel Opoku Manu , Adepeju Deborah Bello; Adeniji Omotayo Leo , Chioma Emmanuel Ukatu; Nonso Okika "Enhancing Know Your Customer (KYC) and Anti-Money Laundering (AML) Compliance Using Blockchain: A Business Analysis Approach" Iconic Research And Engineering Journals, 8(9)

[13] A. A. Varfolomeev and L. H. Al-Farhani, "Blockchain-based digital identity management system for smart city services," in *2023 Int. Conf. Inf. Technol., Appl. Math. Stat. (ICITAMS)*, pp. 79–85, 2023. doi: 10.1109/ICITAMS57610.2023.10525393.

[14] M. Htet, P. T. Yee, and J. R. Rajasekera, "Blockchain-based digital identity management system: A case study of Myanmar," in *2020 Int. Conf. Adv. Inf. Technol. (ICAIT)*, pp. 42–47, 2020. doi: 10.1109/ICAIT51105.2020.9261785.

[15] M. Rachmadhani, T. Immawan, A. Mansur, and W. Choi, "Risk management framework design based on ISO 31000 and SCOR model," Spektrum Ind., vol. 21, no. 1, pp. 41–51, 2023. doi: 10.12928/si.v21i1.93.

[16] B. Alamri, K. Crowley, and I. Richardson, "Cybersecurity risk management framework for blockchain identity management systems in Health IoT," Sensors, vol. 23, no. 1, p. 218, 2023. doi: 10.3390/s23010218.
[17] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: A survey," Wireless Networks, vol. 27, no. 2, pp. 1515–1555, 2021.

[18] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain-based IoT systems: Integration issues, prospects, challenges, and future research directions," Future Generation Computer Systems, vol. 97, pp. 512–529, 2019.

[19] S. Barik and K. G. S. Venkatesan, "Analysis of cybersecurity standard and framework components," Industrial Engineering Journal, vol. 50, no. 6-1, 2021.

[20] Makaš, "Governance, risk, and compliance frameworks applicability in organizations," International Journal of Science and Research Archive, vol. 10, no. 2, pp. 716–724, 2023.

[21] E. Cayirci and A. S. de Oliveira, "Modelling trust and risk for cloud services," Journal of Cloud Computing, vol. 7, Art. no. 14, 2018, doi: 10.1186/s13677-018-0118-0.

[22] R. Beck, C. Mueller-Bloch, and J. King, "Governance in the blockchain economy: A framework and research agenda," Journal of the Association for Information Systems, vol. 19, pp. 1020–1034, 2018, doi: 10.17705/1jais.00518.

[23] T. Polcumpally, K. K. Pandey, A. Kumar, and A. Samadhiya, "Blockchain governance and trust: A multi-sector thematic systematic review and exploration of future research directions," Heliyon, vol. 10, no. 12, Art. no. e32975, 2024, doi: 10.1016/j.heliyon.2024.e32975.

[24] G. Laatikainen, M. Li, and P. Abrahamsson, "A system-based view of blockchain governance," Information and Software Technology, vol. 157, Art. no. 107149, 2023, doi: 10.1016/j.infsof.2023.107149.

[25] M. El Khatib, A. Al Mulla, and W. Al Ketbi, "The role of blockchain in e-governance and decision-making in project and program management," Advances in Internet of Things, vol. 12, no. 3, 2022, doi: 10.4236/ait.2022.123006.

[26] S. Verma and A. Sheel, “Blockchain for government organizations: Past, present and future,” Journal of Global Operations and Strategic Sourcing, vol. 15, no. 3, pp. 406–430, 2022, doi: 10.1108/JGOSS-08-2021-0063.

[27] G. Zyskind and O. Nathan, “Decentralizing privacy: Using blockchain to protect personal data,” in Proc. IEEE Security Privacy Workshops, San Jose, CA, USA, 2015, pp. 180–184.

[28] K. Wüst and A. Gervais, “Do you need a blockchain?,” in Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT), Zug, Switzerland, 2018, pp. 45–54, doi: 10.1109/CVCBT.2018.00011.

[29] N. Atzei, M. Bartoletti, and T. Cimoli, “A survey of attacks on Ethereum smart contracts,” Cryptology ePrint Archive: Report 2016/1007, 2016. [Online]. Available: https://eprint.iacr.org/2016/1007

[30] H. Zhou, A. Milani Fard, and A. Makanju, “The state of Ethereum smart contracts security: Vulnerabilities, countermeasures, and tool support,” Journal of Cybersecurity and Privacy, vol. 2, no. 2, pp. 358–378, 2022, doi: 10.3390/jcp2020019.

[31] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, “Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications, and opportunities,” IEEE Access, vol. 7, pp. 61703–61725, 2019, doi: 10.1109/ACCESS.2019.2925010.

[32] G. Tripathi, M. A. Ahad, and G. Casalino, “A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges,” Decision Analytics Journal, vol. 9, Art. no. 100344, 2023.

[33] D. Commey, B. Mai, S. Hounsinou, and G. Crosby, “Securing blockchain-based IoT systems: A review,” IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3428490.

[34] G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, “Emerging trends in blockchain technology and applications: A review and outlook,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 9, pp. 6719–6742, 2022.

[35] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, “Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing,” Future Internet, vol. 14, no. 11, Art. no. 341, 2022, doi: 10.3390/fi14110341.

[36] S. Hassan and P. De Filippi, “Decentralized autonomous organization,” Internet Policy Review, vol. 10, no. 2, pp. 1–10, 2021, doi: 10.14763/2021.2.1556.

[37] M. Pilkington, “Blockchain technology: Principles and applications,” in Research Handbook on Digital Transformations, F. X. Olleros and M. Zhegu, Eds., Cheltenham, UK: Edward Elgar Publishing, 2016, pp. 225–253.

[38] C. Santana and L. Albareda, “Blockchain and the emergence of decentralized autonomous organizations (DAOs): An integrative model and research agenda,” Technological Forecasting and Social Change, vol. 182, Art. no. 121806, 2022, doi: 10.1016/j.techfore.2022.121806.

[39] F. Wang and P. De Filippi, “Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion,” Frontiers in Blockchain, vol. 2, 2020. [Online]. Available: https://doi.org/10.3389/fbloc.2019.00028

[40] R. Belen-Saglam, E. Altuncu, Y. Lu, and S. Li, “A systematic literature review of the tension between the GDPR and public blockchain systems,” Blockchain: Research and Applications, vol. 4, no. 2, p. 100129, 2023.

[41] [40] B. C. Ghosh, V. Ramakrishna, C. Govindarajan, D. Behl, D. Karunamoorthy, E. Abebe, and S. Chakraborty, “Decentralized cross-network identity management for blockchain interoperation,” arXiv preprint, 2021. [Online]. Available: https://arxiv.org/abs/2104.03277

[42] K. Proctor, “Decentralization, immutability, and integrity: The role of blockchain technology in enhancing cybersecurity,” 2024. [Online]. Available: https://doi.org/10.121296/KBP.30606

[43] J.-P. A. Yaacoub, H. N. Noura, and O. Salman, “Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions,” Internet of Things and Cyber-Physical Systems, vol. 3, pp. 155–179, 2023.

[44] D. Van Roijen, “The European digital identity wallet: A healthcare perspective,” Blockchain in Healthcare Today, vol. 7, 2024. [Online]. Available: https://doi.org/10.30953/bhty.v7.344

[45] K. Duan, G. Pang, and Y. Lin, “Exploring the current status and future opportunities of blockchain technology adoption and application in supply chain management,” Journal of Digital Economy, vol. 2, pp. 244–288, 2023.

[46] O. Rikken, M. Janssen, and Z. Kwee, “Governance challenges of blockchain and decentralized autonomous organizations,” Information Polity, vol. 24, pp. 1–21, 2019. [Online]. Available: https://doi.org/10.3233/IP-190154

[47] L. George and J. Kizhakkethottam, “A comparative study of zero-knowledge proof and homomorphic encryption in guaranteeing data privacy in blockchain applications,” International Journal of Advanced Research, vol. 9, pp. 359–361, 2021. [Online]. Available: https://doi.org/10.21474/IJAR01/12455

[48] B. Pillai, K. Biswas, and V. Muthukkumarasamy, “Cross-chain interoperability among blockchain-based systems using transactions,” The Knowledge Engineering Review, vol. 35, 2020. [Online]. Available: https://doi.org/10.1017/S0269888920000314

[49] L. Alevizos, “Automated cybersecurity compliance and threat response using AI, blockchain, and smart contracts,” International Journal of Information Technology, vol. 17, pp. 767–781, 2025. [Online]. Available: https://doi.org/10.1007/s41870-024-02324-9

[50] H. Han, R. K. Shiwakoti, R. Jarvis, C. Mordi, and D. Botchie, “Accounting and auditing with blockchain technology and artificial intelligence: A literature review,” International Journal of Accounting Information Systems, vol. 48, p. 100598, 2023.

[51] A. Balakrishnan, V. Jain, P. Chintale, S. Gadiparthi, and M. Najana, “Blockchain empowerment in sanctions and AML compliance: A transparent approach,” International Journal of Computer Trends and Technology, 2024. [Online]. Available: https://ssrn.com/abstract=4842695

[52] M. Xin, “A mixed encryption algorithm used in Internet of Things security transmission system,” in Proc. IEEE CyberC Conf., 2015, pp. 62–65. [Online]. Available: https://doi.org/10.1109/CyberC.2015.9

[53] D. Hariyani, P. Hariyani, S. Mishra, and M. K. Sharma, “A literature review on transformative impacts of blockchain technology on manufacturing management and industrial engineering practices,” Green Technologies and Sustainability, vol. 3, no. 3, p. 100169, 2025.

[54] S. Kraus, S. Durst, J. J. Ferreira, P. Veiga, N. Kailer, and A. Weinmann, “Digital transformation in business and management research: An overview of the current status quo,” International Journal of Information Management, vol. 63, p. 102466, 2022.

[55] M. Godyn, M. Kedziora, Y. Ren, Y. Liu, and H. Song, “Analysis of solutions for a blockchain compliance with GDPR,” Scientific Reports, vol. 12, p. 15021, 2022. [Online]. Available: https://doi.org/10.1038/s41598-022-19341-y