ALUPE UNIVERSITY MULTIDISCIPLINARY RESEARCH JOURNAL

ALUPE UNIVERSITY MULTIDISCIPLINARY RESEARCH JOURNAL

journal website: aujournal.au.ac.ke

A Publication of Alupe University

ALUPE UNIVERSITY
Bastion of Knowledge

DOI: https://doi.org/10.65466/9arkq638

eISSN: 3106-0013

Enhancing data integrity in governance of collaborative research: Blockchain, regulatory compliance, and challenges in Kenya and Africa

Tobias Okumu Otibine*[1] and Michael Shinachi Wanyonyi [1]

1. Department of Physics, Mathematics & Computer Sciences, Alupe University. P.O Box 845–50400. Busia, Kenya

ARTICLE INFO

KEYWORDS

Data Integrity; Blockchain Governance; Collaborative Research; Regulatory Compliance; Agricultural Data Systems

ABSTRACT

The increasing reliance on data-intensive collaborative research has intensified concerns regarding data integrity, governance, and regulatory compliance, particularly in multi-institutional and cross-border environments. This study critically examines how blockchain technology can enhance data integrity within collaborative research governance, with a focus on Kenya Agricultural and Livestock Research Organization (KALRO) and comparative African contexts. A qualitative systematic review methodology was employed, drawing on peer-reviewed journal articles (2022–2025) sourced from Scopus, Web of Science, African Journals Online (AJOL), and Google Scholar. Inclusion criteria focused on studies addressing blockchain, data governance, and regulatory compliance in research and data-intensive environments. Findings indicate that key challenges to data integrity include inconsistent data validation, fragmented data systems, jurisdictional regulatory conflicts, and weak enforcement of governance frameworks. While blockchain presents opportunities through immutability, traceability, and decentralized control, its application introduces tensions with legal frameworks such as the Kenya Data Protection Act (2019) and the General Data Protection Regulation, particularly regarding the right to erasure. Evidence from Kenyan and broader African studies demonstrates that permissioned blockchain systems, combined with smart contracts, can enhance auditability, enforce compliance, and mitigate disputes over data ownership in collaborative research. The study concludes that blockchain is not a standalone solution but a complementary governance tool that must be integrated with robust legal, institutional, and technical

*Corresponding author: Tobias Okumu Otibine Email: tokumu@au.ac.ke

frameworks. It recommends the development of standardized data governance protocols, regulatory harmonization across jurisdictions, and capacity building within research institutions to ensure sustainable adoption.

Introduction

Collaborative research has increasingly become the cornerstone of scientific advancement in the twenty-first century, particularly in data-intensive fields such as agricultural science, public health, environmental studies, and biotechnology (Grossman *et al.,* 2024; Ugochukwu & Phillips, 2024). In Africa, and specifically in Kenya, institutions such as the Kenya Agricultural and Livestock Research Organization (KALRO) play a central role in coordinating multi-stakeholder research initiatives involving government agencies, universities, international donors, and private sector actors (Chichaibelu *et al.,* 2023). These collaborations are essential in addressing complex challenges such as food insecurity, climate change adaptation, and sustainable agricultural productivity. However, the expansion of collaborative research has simultaneously intensified concerns regarding data integrity, governance, and regulatory compliance (Nielsen *et al.,* 2025).

Data integrity, defined as the accuracy, consistency, completeness, and reliability of data throughout its lifecycle, is fundamental to the credibility and reproducibility of research outcomes (Hussain *et al.,* 2024). In collaborative environments, where multiple actors contribute to data generation, processing, storage, and analysis, maintaining data integrity becomes increasingly complex. Empirical studies demonstrate that inconsistencies in data validation protocols, heterogeneous data formats, and fragmented data management systems significantly undermine the quality and reliability of shared datasets (Aldoseri *et al.,* 2023; Nielsen *et al.,* 2024). These challenges are particularly pronounced in African research ecosystems, where infrastructural disparities, limited standardization, and varying institutional capacities exacerbate data governance weaknesses (Chichaibelu *et al.,* 2023; Nyachiro *et al.,* 2023). In the Kenyan context, KALRO operates within a highly networked research environment that involves both national and international partnerships. These collaborations often require the sharing of large datasets across institutional and jurisdictional boundaries, introducing challenges related to interoperability, access control, and accountability (Grossman *et al.,* 2024; Nyachiro *et al.,* 2023). For instance, agricultural research projects involving genomic data, climate data, and farmer-level socio-economic data frequently encounter inconsistencies arising from divergent data collection methodologies and storage systems. Such inconsistencies not only compromise data integrity but also reduce the efficiency of collaborative research efforts (Numajiri & Hayashi, 2024).

Beyond technical challenges, regulatory frameworks introduce an additional layer of complexity in data governance. The Kenya Data Protection Act of 2019 establishes strict requirements for the collection, processing, storage, and transfer of personal data (GoK 2019). While the Act aligns with international standards such as the General Data Protection Regulation (GDPR), its implementation within collaborative research contexts presents significant operational challenges (Chichaibelu *et al.,* 2023). Cross-border research collaborations often involve jurisdictions with differing legal requirements, creating conflicts that hinder seamless data sharing (Ugochukwu & Phillips, 2024). For example, GDPR provisions such as the "right to be forgotten" are inherently incompatible with certain technological systems that rely on permanent data records, thereby

complicating compliance in multi-jurisdictional research environments (Charles *et al.,* 2024).

The intersection of data governance and regulatory compliance is further complicated by issues of data ownership and intellectual property rights. In collaborative research projects, multiple stakeholders often have competing interests regarding the ownership, access, and commercialization of data (Ugochukwu & Phillips, 2024). In the absence of clearly defined governance frameworks, these conflicts can lead to disputes that disrupt research continuity and undermine trust among collaborators. African studies on data sharing practices highlight that inequities in data ownership and access disproportionately affect local research institutions, particularly when collaborating with international partners (Chichaibelu *et al.,* 2023).

Technological advancements have been proposed as potential solutions to these challenges, with blockchain technology emerging as a particularly promising innovation. Blockchain is a decentralized distributed ledger system that enables secure, transparent, and immutable recording of transactions (Wen *et al.,* 2023). Its core features immutability, transparency, decentralization, and traceability—position it as a viable tool for enhancing data integrity and governance in collaborative research environments (Hussain *et al.,* 2024). In particular, permissioned blockchain systems, which restrict access to authorized participants, offer a controlled environment suitable for institutional applications such as research data management (Saleh, 2024).

In the context of KALRO and similar African institutions, blockchain technology has the potential to address key challenges associated with data integrity and governance. By providing a tamper-resistant record of data transactions, blockchain can enhance data provenance, ensuring that all modifications to data are traceable and verifiable (Hussain *et al.,* 2024; Wen *et al.,* 2023). Smart contracts-self-executing agreements embedded within blockchain systems can automate compliance with regulatory requirements and enforce governance rules, thereby reducing the risk of human error and intentional data manipulation (Charles *et al.,* 2024). Furthermore, blockchain's decentralized architecture can mitigate the risks associated with centralized data storage systems, such as single points of failure and unauthorized access (Saleh, 2024).

Despite these potential benefits, the adoption of blockchain technology in collaborative research remains limited, particularly in African contexts (Hamba *et al.,* 2024). Existing literature indicates a significant gap in empirical studies examining the application of blockchain in research data governance, especially within agricultural research institutions (Ugochukwu & Phillips, 2024). Moreover, the interaction between blockchain technology and existing regulatory frameworks remains underexplored, raising questions about its practical feasibility and legal compatibility (Charles *et al.,* 2024). This study seeks to address these gaps by critically examining the role of blockchain technology in enhancing data integrity within collaborative research governance. It focuses on KALRO as a primary case study while integrating comparative insights from other African research contexts. The study aims to provide a comprehensive analysis of the challenges associated with data integrity and governance in collaborative research and to evaluate the extent to which blockchain technology can address these challenges within existing regulatory frameworks. By doing so, it contributes to the growing body of literature on data governance and technological innovation in research environments, with particular relevance to developing regions.

Methodology and Materials

This study adopts a qualitative systematic review design to critically synthesize existing scholarly literature on data integrity, blockchain technology, and data governance in collaborative research environments. The systematic review approach was selected due to its suitability in consolidating diverse perspectives, identifying knowledge gaps, and generating evidence-based insights in emerging research domains (Aldoseri *et al.,* 2023; Numajiri & Hayashi, 2024). The data collection process involved a comprehensive search of peer-reviewed journal articles published between 2022 and 2025 to ensure the relevance and currency of the findings. The primary databases used in this study included Scopus, Web of Science, African Journals Online (AJOL), and Google Scholar. These databases were selected due to their extensive coverage of high-quality academic publications across global and regional contexts (Grossman *et al.,* 2024). Search terms included combinations of keywords such as "data integrity," "data governance," "blockchain," "collaborative research," "regulatory compliance," and "Africa." Boolean operators were used to refine the search and enhance the precision of results.

The inclusion criteria for the study required that selected articles: (i) focus on data governance, data integrity, or blockchain applications; (ii) address collaborative, institutional, or cross-border data environments; (iii) be published in peer-reviewed journals; and (iv) include verifiable Digital Object Identifiers (DOIs) (Chichaibelu *et al.,* 2023). Additionally, the study ensured a balanced representation of sources, with approximately 30% drawn from Kenyan studies, 30% from broader African contexts, and 40% from global literature. This distribution was intended to provide both contextual relevance and theoretical depth (Hamba *et al.,* 2024). Exclusion criteria were applied to eliminate non-scholarly sources, including blog posts, opinion pieces, conference abstracts without full papers, and publications lacking methodological rigor. Articles published prior to 2022 were excluded to maintain alignment with current developments in data governance and blockchain technology (Wen *et al.,* 2023). Duplicates and studies with limited relevance to the research objectives were also removed during the screening process.

The initial search yielded over 120 articles. These were subjected to a multi-stage screening process involving title review, abstract evaluation, and full-text assessment. Following this process, 28 articles were selected for detailed analysis. The selected studies were then subjected to thematic analysis, which involved coding and categorizing data into key themes related to data integrity challenges, technological barriers, regulatory compliance, and blockchain-based solutions (Hussain *et al.,* 2024). The thematic analysis process was both inductive and deductive. Inductive coding allowed for the identification of emerging themes from the data, while deductive coding was guided by the study's conceptual framework, which focuses on the intersection of data integrity, governance, and technology. This approach enabled a comprehensive analysis of the literature, capturing both established and emerging trends in the field (Numajiri & Hayashi, 2024).

To enhance the validity and reliability of the findings, the study employed triangulation by integrating insights from multiple sources and contexts (Grossman *et al.,* 2024). Particular attention was given to studies focusing on African research environments to ensure contextual relevance (Chichaibelu *et al.,* 2023). Additionally, the analysis incorporated institutional perspectives, including the operational context of KALRO, to ground the findings in practical realities (Hamba *et al.,* 2024). Ethical considerations were observed throughout the study by ensuring proper citation and acknowledgment of all sources in accordance with APA 7th edition guidelines. The study did not involve primary data collection

involving human participants and therefore did not require ethical clearance.

Results and Discussion of Findings

Overview of Thematic Findings

The systematic review revealed that data integrity challenges in collaborative research are not isolated technical deficiencies but are embedded within broader socio-technical and regulatory systems. Four dominant and interrelated themes emerged: (i) systemic weaknesses in data integrity practices, (ii) technological and infrastructural constraints, (iii) regulatory and ethical governance challenges, and (iv) the role of blockchain as a socio-technical governance mechanism. Unlike purely technical interpretations of data integrity, the findings align with contemporary scholarship that frames data integrity as a governance problem shaped by institutional practices, technological infrastructures, and ethical norms (Hussain *et al.,* 2024; Nielsen *et al.,* 2024). This perspective is consistent with emerging literature in data governance studies, which emphasizes that integrity is not merely about accuracy, but about trustworthiness, accountability, and legitimacy across the data lifecycle.

Data Integrity as a Systemic Governance Challenge

Inconsistent Data Validation and Epistemic Fragmentation

The findings demonstrate that inconsistent data validation practices remain a central threat to integrity in collaborative research. Across the reviewed literature, there is consensus that multi-institutional collaborations introduce epistemic fragmentation, where different actors apply divergent standards of data collection, cleaning, and validation (Aldoseri *et al.,* 2023; Numajiri & Hayashi, 2024). This fragmentation is particularly pronounced in interdisciplinary environments such as agricultural research, where datasets combine biophysical, socio-economic, and environmental variables. In such contexts, the absence of standardized validation frameworks leads to what Grossman *et al.* (2024) describe as "structural inconsistencies in data architectures," which compromise interoperability and analytical coherence. The implication is that data integrity cannot be achieved solely through post hoc validation mechanisms. Rather, it requires institutionalized standardization protocols embedded at the point of data generation. This aligns with the broader literature on research reproducibility, which emphasizes that integrity must be designed into data systems rather than retrospectively imposed.

Data Provenance and the Problem of Trust in Distributed Systems

A recurring finding is the weakness of data provenance mechanisms in collaborative environments. Provenance, the ability to trace the origin and transformation of data is central to establishing trust in shared datasets. However, the review indicates that most research systems rely on fragmented and manual documentation practices, which are prone to error and manipulation. From a theoretical perspective, this challenge reflects what scholars in information systems describe as the "trust deficit" in distributed data ecosystems (Wen *et al.,* 2023). When multiple actors interact with data across institutional boundaries, the absence of reliable provenance mechanisms creates uncertainty regarding authenticity and accountability.

In KALRO-related collaborations, for example, datasets may be modified by different stakeholders over time without a unified audit trail. This leads to ambiguity regarding data ownership, authorship, and validity. Such conditions undermine not only data integrity but also epistemic trust, which is essential for collaborative knowledge production.

Data Ownership, Power Asymmetries, and Ethical Implications

The findings further reveal that data integrity is closely tied to issues of ownership and power. In collaborative

research, particularly in African contexts, there are often asymmetries between local institutions and international partners. These asymmetries influence who controls data, how it is used, and whose interests it serves (Chichaibelu *et al.,* 2023). From an ethical standpoint, this raises concerns about data justice and equitable participation in knowledge production. Scholars argue that when data ownership is concentrated among dominant actors, it can lead to selective reporting, restricted access, or even data manipulation, all of which compromise integrity (Ugochukwu & Phillips, 2024). This finding reinforces the argument that data integrity must be understood not only as a technical property but also as an ethical and political construct**,** shaped by governance arrangements and institutional power dynamics.

Technological Constraints and Their Implications for Integrity

Interoperability Failures and Fragmented Data Ecosystems

The review identifies interoperability as a critical technological barrier. Research institutions typically operate heterogeneous systems that lack standardized communication protocols, resulting in fragmented data ecosystems. This fragmentation leads to duplication, inconsistencies, and data silos, which collectively undermine integrity. As noted by Grossman *et al.* (2024), the absence of interoperable frameworks creates "data friction," where the cost of integrating datasets exceeds the benefits of collaboration.

In practical terms, KALRO's multi-platform data environment exemplifies this challenge. Data generated by different partners may be stored in incompatible formats, making integration difficult and increasing the likelihood of errors during data transformation processes.

Limitations of Cloud Computing in Governance Contexts

While cloud computing has enhanced data accessibility and scalability, the findings indicate that it introduces new governance challenges. These include vulnerabilities to breaches, uncertainties around data sovereignty, and difficulties in enforcing consistent access control policies. From a governance perspective, cloud systems represent a form of centralized trust architecture**,** where integrity depends on the reliability of service providers. However, scholars argue that such centralized models are inherently limited in multi-stakeholder environments, where trust must be distributed rather than concentrated (Li *et al.,* 2021).

Version Control and the Problem of Data Fluidity

Version control challenges further complicate data integrity. As datasets evolve, multiple versions may coexist, creating confusion about which version is authoritative. This issue reflects what information science literature describes as "data fluidity," where continuous updates blur the boundaries between stable and dynamic datasets. Although tools such as Git provide technical solutions, their limited adoption in research contexts highlights a broader issue: the lack of integration between technical tools and governance frameworks**.**

Regulatory and Ethical Governance Challenges

Jurisdictional Complexity and Regulatory Fragmentation

The findings highlight significant challenges arising from overlapping regulatory frameworks. Collaborative research often involves compliance with multiple legal regimes, including national laws such as the Kenya Data Protection Act 2019 (GoK, 2019). This regulatory fragmentation creates what scholars' term "jurisdictional misalignment," where conflicting legal requirements hinder data sharing and governance (Charles *et al.,* 2024). For example, GDPR's right to erasure conflicts with systems that require permanent data records, creating legal and operational tensions.

Ethical Governance and the Limits of Consent

Ethical challenges related to informed consent are also prominent. In large-scale collaborative projects, obtaining and maintaining valid consent across multiple uses of data is complex. This is particularly relevant in longitudinal studies, where data may be reused beyond its original purpose. From an ethical standpoint, this raises questions about participant autonomy, transparency, and accountability. Scholars argue that traditional consent models are inadequate for dynamic data ecosystems, necessitating more adaptive governance mechanisms.

Governance Gaps and Institutional Weaknesses

The review indicates that existing governance frameworks are often fragmented and weakly enforced. This results in inconsistent application of policies, undermining accountability and integrity. This finding aligns with broader literature on African research systems, which highlights institutional capacity constraints as a key barrier to effective data governance (Nyachiro *et al.,* 2023).

Blockchain as a Socio-Technical Governance Mechanism

Reframing Blockchain Beyond Technology

A key insight from the analysis is that blockchain should not be viewed merely as a technical tool but as a socio-technical governance mechanism. Its value lies in its ability to restructure trust relationships, redistribute authority, and embed governance rules within technological systems. This perspective is consistent with recent scholarship that conceptualizes blockchain as an "institutional technology" capable of enforcing rules without centralized intermediaries (Wen *et al.,* 2023).

Enhancing Data Provenance and Auditability

Blockchain's most significant contribution to data integrity lies in its ability to provide immutable and transparent audit trails. By recording all data transactions on a distributed ledger, blockchain enables traceability and accountability across the data lifecycle. Empirical studies such as SciChain by Al-Mamun *et al.* (2021) demonstrate how blockchain can enhance provenance in scientific workflows. This directly addresses the trust deficit identified earlier, by providing verifiable evidence of data origin and transformation.

Permissioned Blockchain as the Preferred Model

The findings strongly support the adoption of permissioned blockchain systems in research contexts. Unlike permissionless systems, which are open and decentralized, permissioned systems restrict access to authorized participants, enabling controlled governance. This distinction is critical. While permissionless blockchains offer transparency, they pose risks related to anonymity, lack of control, and regulatory non-compliance. In contrast, permissioned systems align more closely with institutional requirements, allowing for role-based access control, regulatory compliance, and governance oversight.

Smart Contracts and Automated Ethical Compliance

Smart contracts represent another key innovation. These programmable agreements can enforce governance rules automatically, reducing reliance on manual processes. From an ethical perspective, smart contracts can operationalize principles such as:

- informed consent,
- data access restrictions,
- compliance with legal frameworks.

This aligns with emerging literature on "ethics by design," where ethical principles are embedded within technological systems rather than applied externally.

Ethical and Governance Implications of Blockchain

Immutability vs. the Right to Erasure

One of the most significant ethical tensions identified is the conflict between blockchain immutability and the right to erasure. While immutability enhances integrity,

it limits the ability to modify or delete data, raising concerns about compliance with data protection laws. This tension reflects a broader debate in the literature regarding the compatibility of blockchain with human rights-based data governance frameworks.

Algorithmic Governance and Accountability

Blockchain introduces new forms of governance based on algorithms and code. While this enhances efficiency, it raises questions about accountability. If governance rules are embedded in code, who is responsible when those rules produce unintended outcomes? Scholars argue that algorithmic governance must be complemented by institutional oversight mechanisms to ensure accountability and ethical compliance.

Risks and Limitations of Blockchain

Security Vulnerabilities

Blockchain systems are vulnerable to attacks such as Sybil and 51% attacks. While these risks are lower in permissioned systems, they remain relevant, particularly in contexts with limited technical capacity.

Scalability and Infrastructure Constraints

Scalability remains a major challenge, particularly for data-intensive research. Blockchain systems may struggle to handle large datasets, necessitating hybrid architectures that combine blockchain with traditional databases.

Institutional and Capacity Barriers

The adoption of blockchain requires significant technical expertise and infrastructure. In African research contexts, these requirements may pose substantial barriers.

Towards Integrated Data Governance

The findings suggest that data integrity in collaborative research requires an integrated approach that combines:

- standardized data governance frameworks,
- interoperable technological systems,
- adaptive regulatory mechanisms,
- and blockchain-enabled trust infrastructures.

Blockchain plays a critical role, but only as part of a broader governance ecosystem.

Conclusion

This section demonstrates that data integrity challenges in collaborative research are deeply rooted in systemic, technological, and ethical factors. Blockchain offers transformative potential by enhancing transparency, traceability, and accountability. However, its effectiveness depends on careful integration with governance frameworks, regulatory systems, and institutional capacities. Ultimately, achieving data integrity requires a holistic governance approach that balances technological innovation with ethical and regulatory considerations.

Furthermore, this study establishes that data integrity remains a critical challenge in collaborative research environments, particularly within African contexts characterized by fragmented systems, evolving governance frameworks, and regulatory complexities. Structural weaknesses in data management, coupled with inconsistencies in validation and limited data provenance mechanisms, significantly undermine the reliability and reproducibility of research outputs (Nielsen *et al.,* 2024; Grossman *et al.,* 2024). The findings further demonstrate that regulatory frameworks, while essential for safeguarding data privacy and ethical standards, introduce significant operational challenges in cross-border research collaborations. Legal fragmentation and conflicts between regulatory provisions and emerging technologies complicate compliance and hinder efficient data sharing (Charles *et al.,* 2024; Chichaibelu *et al.,* 2023).

Blockchain technology offers a promising pathway for enhancing data integrity through its features of immutability, transparency, and decentralized control.

However, its adoption is constrained by technical, regulatory, and institutional challenges. The study concludes that blockchain is not a standalone solution but a complementary tool that must be integrated within broader governance frameworks. Ultimately, improving data integrity in collaborative research requires a holistic approach that combines technological innovation with institutional reform, regulatory harmonization, and capacity development.

Recommendations

To address the challenges identified in this study and to enhance data integrity in collaborative research environments, several strategic recommendations are proposed. First, research institutions should develop and implement standardized data governance frameworks that prioritize data integrity, interoperability, and accountability. Such frameworks should include clearly defined protocols for data collection, validation, storage, and sharing, ensuring consistency across collaborating entities. Evidence from recent studies indicates that standardized data governance significantly improves data quality and reduces inconsistencies in multi-institutional research projects (Aldoseri *et al.,* 2023; Numajiri & Hayashi, 2024).

Second, policymakers should prioritize the harmonization of data protection regulations across African jurisdictions. The current fragmentation of legal frameworks creates barriers to cross-border research collaboration and increases compliance risks. Regional bodies and governments should work towards developing unified regulatory standards that facilitate data sharing while maintaining high levels of data protection (Chichaibelu *et al.,* 2023). Harmonization efforts should also address the emerging challenges posed by new technologies such as blockchain, ensuring that legal frameworks remain relevant and adaptable.

Third, research institutions such as KALRO should consider the adoption of permissioned blockchain systems as part of their data governance strategies. These systems offer a controlled environment for secure data sharing, enabling institutions to maintain oversight while benefiting from blockchain's features of transparency and immutability (Hamba *et al.,* 2024; Ondiek & Onyango, 2024). The integration of smart contracts can further enhance compliance by automating governance processes and reducing reliance on manual oversight.

Author contribution

Conceptualization; Methodology; Formal analysis; Investigation; Writing – original draft; Writing – review and editing; Project administration.

Acknowledgement

AI was used to condense the manuscript to have less than 5700 words. Secondly, it was used for editing and grammar correction and improve the general presentation of the paper.

Conflict of Interest

There was no conflict of interest to declare.

References

Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2023). Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges. *Applied Sciences*, *13*(12), 7082. https://doi.org/10.3390/app13127082

Al-Mamun, A., Yan, F., & Zhao, D. (2021). SciChain: Blockchain-enabled Lightweight and Efficient Data Provenance for Reproducible Scientific Computing. In *2021 IEEE 37th International Conference on Data Engineering (ICDE)* (pp. 1853–1858). IEEE. https://doi.org/10.1109/ICDE51399.2021.00166

Charles, W. M., Waal, M. B. van der, Flach, J., Bisschop, A., Waal, R. X. van der, Es-Sbai, H., & McLeod, C. J. (2024). Blockchain-Based Dynamic Consent and its Applications for Patient-Centric Research and Health Information Sharing: Protocol for an Integrative Review. *JMIR Research Protocols*, *13*(1), e50339. https://doi.org/10.2196/50339

Chichaibelu, B. B., Baumüller, H., & Matschuck, M. A. (2023). Protecting the data of African agricultural producers: A review of national laws, compliance and perceptions. *Law, Innovation and Technology*, *15*(2), 617–661. https://doi.org/10.1080/17579961.2023.2245673

GoK. (2019). The Data Protection Act [Laws of Kenya]. *Government of Kenya*. Retrieved from https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf

Grossman, R. L., Boyles, R. R., Davis-Dusenbery, B. N., Haddock, A., Heath, A. P., O'Connor, B. D., Resnick, A. C., Taylor, D. M., & Ahalt, S. (2024). A Framework for the Interoperability of Cloud Platforms: Towards FAIR Data in SAFE Environments. *Scientific Data*, *11*(1), 241. https://doi.org/10.1038/s41597-024-03041-5

Hamba, L. A., Kangethe, B. M., & Odoyo, W. O. (2024). Empowering Sustainable Startups in Kenya Through Blockchain Technology. *IC-ITECHS*, *5*(1), 1035–1038. https://doi.org/10.32664/ic-itechs.v5i1.1682

Hussain, M. I., Bhuiyan, K. I., Sumon, S. A., Akter, S., Hossain, M. I., & Akther, A. (2024). Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) through Blockchain Technology: A Comprehensive Approach. *Advances in Artificial Intelligence and Machine Learning; Review*, *4*(4), 2883–2907.

Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. (2021). Blockchain-based trust management in cloud computing systems: A taxonomy, review and future directions. *Journal of Cloud Computing*, *10*(1), 1–34. https://doi.org/10.1186/s13677-021-00247-5

Nielsen, J., Flanagan, M., Gurrin, L. C., Thornton, J., & Mol, B. W. (2025). Concerns about data integrity across 263 papers by one author. *Journal of Gynecology Obstetrics and Human Reproduction*, *54*(6), 102794. https://doi.org/10.1016/j.jogoh.2024.102794

Numajiri, H., & Hayashi, T. (2024). Analysis on open data as a foundation for data-driven research. *Scientometrics*, *129*(10), 6315–6332. https://doi.org/10.1007/s11192-024-04956-x

Nyachiro, A., Ondimu, K., & Mafura, G. (2023). Adoption Strategy for Cloud Computing in Kenyan Research Institutions. *International Journal of Innovative Research and Development*, *12*(2), 42–107. https://doi.org/10.24940/ijird/2023/v12/i2/FEB23001

Ondiek, J. O., & Onyango, G. (2024). Blockchain technologies in digital governance: The Kenyan experience with promoting public accountability. In *The Routledge International Handbook of Public Administration and Digital Governance* (pp. 112–124). Taylor and Francis Inc. https://doi.org/10.4324/9781003458081-9

Saleh, A. M. S. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. *Blockchain: Research and Applications*, *5*(3), 100193. https://doi.org/10.1016/j.bcra.2024.100193

Ugochukwu, A. I., & Phillips, P. W. B. (2024). Open data ownership and sharing: Challenges and opportunities for application of FAIR principles and a checklist for data managers. *Journal of Agriculture and Food Research*, *16*, 101157. https://doi.org/10.1016/j.jafr.2024.101157

Wen, B., Wang, Y., Ding, Y., Zheng, H., Qin, B., & Yang, C. (2023). Security and privacy protection technologies in securing blockchain applications. *Information Sciences*, *645*, 119322. https://doi.org/10.1016/j.ins.2023.119322