ABUAD Journal of Engineering Research and Development (AJERD)
ISSN (online): 2645-2685; ISSN (print): 2756-6811

Volume 7, Issue 2, 475-483

# Review of Blockchain Technology on Data Security and Privacy: Recommendations for Advancing Tanzania's ICT Sector

Lazaro Inon KUMBO, Deogratias Tasilo MAHUWI, Bernad Joseph HAYUMA, Victor Simon NKWERA, Christopher Denis NTYANGIRI, Martin Ludovick MUSHI

*Department of Computing and Communication Technology, National Institute of Transport, Tanzania*
lazaro.kumbo@nit.ac.tz/deogratias.mahuwi@nit.ac.tz/bernad.hayuma@nit.ac.tz/
victor.simon@nit.ac.tz/christopher.ntyangiri@nit.ac.tz/martin.mushi@nit.ac.tz

*Corresponding Author:* deogratias.mahuwi@nit.ac.tz, *+255716311519*
*Date Submitted:* *15/07/2024*
*Date Accepted:* *26/10/2024*
*Date Published:* *28/10/2024*

***Abstract:*** *The rapid growth of the ICT sector has led to increased global data exchange and innovation opportunities. The increased use of technology has brought about concerns regarding data security and privacy which triggered a rising interest in blockchain technology as a potential solution to security challenges. This research endeavours to comprehensively examine the influence of blockchain on data security and privacy inside and outside Tanzanian, filling the gap that exists. The blended approach was used to analyse blockchain's effects while focusing on ethical considerations. The review emphasizes the benefits of blockchain in enhancing data security, trust, and transparency, along with its various applications. The research highlights blockchain technology's potential to offer robust data protection and improve transparency while identifying the challenges that must be addressed for successful implementation. The study investigates the role of blockchain in securing information systems in global and Tanzanian settings, focusing on sectors such as healthcare, banking, education, and land registration. The study emphasises the significant potential of blockchain technology to impact various industries in Tanzania profoundly. It offers valuable insights for professionals, policymakers, and researchers, highlighting the need to investigate how blockchain can be applied explicitly within different sectors. Additionally, it suggests practical strategies for seamlessly integrating this technology, considering the unique challenges the Tanzanian ICT sector encounters.*

***Keywords:*** *Blockchain Technology, Data Security, Data Privacy, Decentralized Systems, Cybersecurity, Information and Communication Technology (ICT).*

## 1. INTRODUCTION

The Information and Communication Technology (ICT) sector has experienced remarkable growth, significantly increasing data production and transfer [1,2]. This surge in data creation presents new opportunities for innovation and efficiency and raises important issues regarding data security and privacy [3]. As cyber threats, data breaches, and unauthorised access continue to rise, there is an urgent need for strong measures to protect sensitive information in the ICT industry.

The invention of Blockchain has emerged among promising solutions to address data security and privacy. Originally developed as the fundamental technology for cryptocurrencies like Bitcoin [4], blockchain has advanced to be applicable in various industries and sectors. Its decentralised and secure characteristics have proven valuable in finance, supply chain management, healthcare, and more. The decentralised, transparent, and tamper-proof features of blockchain offer a revolutionary approach to data management in the ICT sector. Blockchain operates as a decentralised ledger, securely recording and validating transactions across a distributed network of peers, ensuring verification and transparency. Its primary purpose is to enable secure, direct transactions between parties without intermediaries [5-8]. This not only enhances the security and trustworthiness of transactions but also has the potential to streamline processes across multiple industries.

The increasing interest in blockchain technology has prompted the evaluation on how it affects data security and privacy in the ICT sector globally and how it will affect it locally. Existing research and case studies have shed light on the strengths and weaknesses of blockchain in safeguarding data [9,10]. Presently, research in Tanzania lacks practical applications for using blockchain to improve data security and privacy. This study aims to bridge this gap by thoroughly examining how blockchain technology can enhance data security and privacy within Tanzania's industries and organisations. Through an extensive literature review encompassing global perspectives, the research seeks to extrapolate and apply this knowledge to the Tanzanian context, thereby advocating for adopting blockchain technology to fortify data security and privacy measures within Tanzania's ICT sector.

The ICT sector in Tanzania faces specific challenges in ensuring data security and privacy. Issues such as inadequate infrastructure, limited digital literacy, and insufficient regulatory frameworks complicate efforts to safeguard sensitive information. For instance, in sectors like healthcare, data breaches and unauthorised access to patient records are common problems [11]. Blockchain technology could provide a robust solution to these challenges by enhancing the security and integrity of health records. Similarly, the banking sector in Tanzania could benefit from blockchain's ability to secure financial transactions and reduce fraud, addressing the prevalent issues of fund theft and transaction delays [12].

Moreover, blockchain applications in land registration can address transparency and corruption issues. Tanzania's current land registration system is plagued by inefficiencies and fraudulent activities, leading to disputes and property loss [13]. Blockchain's immutable ledger can ensure that land records are tamper-proof and transparently managed, which could significantly reduce corruption and streamline the registration process.

The outcomes of this research effort are expected to offer valuable insights for organisations, researchers, and policymakers, unveiling a deeper understanding of the practical implications of blockchain and potential strategies for its implementation to strengthen data security and privacy within Tanzania's ICT sector. Ultimately, this study aims to equip decision-makers with the necessary information to assess and adopt blockchain solutions effectively. By leveraging the strengths of blockchain, Tanzania has the potential to improve data security and privacy across various sectors, leading to enhanced trust and efficiency in digital transactions.

The research paper presentation has been organized in five numbered sections where some sections contain sub-sections. The sections are Introduction, Literature Review, Methodology, Results and Discussion whereas the last section is Conclusion.

## 2. LITERATURE REVIEW

The research paper's literature review is organised into five parts to investigate how blockchain affects individuals' and organisations' data security and privacy. It discusses blockchain's role in data security, including trustworthiness and transparency, and critical considerations for integrating blockchain technology in security, such as scalability and legal issues.

### 2.1 Blockchain Technology and Data Security

Blockchain has proven innovative and has the extraordinary capability to improve data security in various industries and applications significantly. Its decentralised and immutable fauna guarantees that data recorded on the blockchain remains unchanged and tamper-proof, providing unparalleled security and trust [14,15]. This exceptional attribute of blockchain is regarded as the most resistant to unauthorised alterations of data and information, making it a preferable choice for safeguarding sensitive data in the field of ICT [15-18]. In addition to its immutability, blockchain's utilisation of advanced cryptographic algorithms adds multiple layers of security, further shielding data from unauthorised access and preserving its integrity [18,19]. This powerful combination of blockchain's fundamental characteristics and sophisticated cryptographic techniques makes it an invaluable tool for protecting sensitive information in today's increasingly digital and interconnected world [17].

### 2.2 Trustworthiness and Transparency

Blockchain technology offers a significant advantage in strengthening trust within information systems. Its transparency and consensus mechanisms empower all participants to securely and independently verify and validate data transactions, ensuring that the integrity and authenticity of the data are upheld [15,20]. This characteristic promotes transparency and increased accountability, reducing the jeopardy of data being tampered with and probably unauthorised access. Furthermore, the decentralised nature of blockchain technology diminishes dependence on a single centralised point of Management, thereby decreasing the danger associated with single points of failure [18,21].

### 2.3 Use Cases in Data Security

Blockchain technology has demonstrated considerable potential in enhancing privacy and data security across various industries. One notable application is its capability to deliver a decentralised and secure infrastructure for exchanging and storing private patient information within the healthcare sector [15,22,23]. This innovative approach enhances data management and ensures the confidentiality and integrity of sensitive medical data. In the realm of the Internet of Things (IoT), blockchain technology is crucial in ensuring data integrity and enabling secure communication among interconnected IoT devices [24]. By leveraging its decentralised and immutable ledger, blockchain enhances the trustworthiness of the data exchanged between IoT devices, mitigating the risk of unauthorised access or tampering. This added layer of security provided by blockchain technology is critical for preserving the privacy and reliability of IoT ecosystems. Therefore, the devices can securely exchange data and execute transactions through blockchain, bolstering IoT networks' security and reliability. Furthermore, there is growing attention to leveraging blockchain to fortify the security of cloud storage systems and enhance data privacy [25].

### 2.4 Scalability and Interoperability Challenges

The advantages blockchain offers in guaranteeing data security and privacy are manifold. However, overcoming significant challenges to leverage these advantages is crucial. One of the most pressing issues is scalability. The resource-intensive nature of consensus algorithms in blockchain can result in scalability hurdles, particularly when the technology is required to manage substantial amounts of data [26,27]. The widespread adoption of blockchain hinges on overcoming this

significant hurdle and making it preferable to the current technology. In addition, achieving interoperability between different blockchain platforms and integrating them effectively with current information systems are critical areas of focus for ongoing research and development efforts. Ensuring that various blockchain systems can seamlessly work together and be integrated with existing systems and processes is essential to realize blockchain technology's full potential. These challenges must be carefully addressed to fully leverage the benefits of blockchain technology while ensuring smooth integration into existing systems and processes [26].

### 2.5 Legal and Regulatory Considerations

When considering integrating blockchain technology to enhance data security and privacy, it is crucial to assess the current legal and regulatory frameworks thoroughly. Blockchain records' decentralised and unchangeable nature can significantly impact data governance, ownership, and compliance with privacy regulations [28,29]. As a result, organisations must carefully align their blockchain implementations with existing legal requirements and privacy policies to avoid likely conflicts and guarantee compliance with regulatory standards. This alignment is essential to ensure the security and privacy of data while utilising blockchain technology [29].

The current literature underscores the considerable promise of blockchain in effectively addressing and alleviating security and privacy challenges. Blockchain offers various advantages, including heightened data protection, increased reliability, and greater accountability stemming from its decentralised nature, immutability, and transparency. Nevertheless, it's essential to address scalability, interoperability, and legal challenges for successful deployment. To maximise the benefits of blockchain in enhancing data security and privacy, it's imperative to carefully assess its relevance and implications within specific ICT environments.

## 3. METHODOLOGY

In this research study, the methodology section serves as a vital guide, providing a comprehensive overview of the precise steps to accomplish the research goals. This section meticulously delineates the systematic approach for gathering, analysing, and interpreting data, thus ensuring the study's credibility and dependability. Encompassing everything from the research design to the tools used for data collection, the statistical methodologies applied, and the ethical considerations upheld, this section offers a transparent and detailed perspective on the framework underpinning the investigation. This transparency not only enhances the clarity of the study but also facilitates the reproducibility of the scientific inquiry.

### 3.1 Research Design

The study utilised a comprehensive mixed-methods approach to evaluate the influence of blockchain on data security and privacy. Integrating quantitative and qualitative methods, the research conducted a thorough analysis encompassing theoretical perspectives and empirical evidence. The qualitative method was used in collecting information from the papers while quantitative methods were used to summarize the findings. This combined approach allowed for a more in-depth examination of the subject matter.

### 3.2 Sample Method

The research was centred on investigating information security and cybersecurity, explicitly focusing on the potential impact of blockchain technology in safeguarding information systems. The study involved an in-depth analysis of academic papers published over seven years, from 2016 to 2023. Selection criteria for the documents included rigorous peer review and exclusion from predatory publisher lists to ensure the quality and reliability of the sources. Given the significant security breaches affecting multinational entities during this timeframe, the research delved into 45 publications to examine blockchain's role in fortifying information systems' security. For specific details regarding the sources of these publications, please refer to Table 1 which shows the Publication Sources versus Frequency where, Publication Source refers to the place where publication was obtained and Frequency refers to the number of publications referred.

### 3.3 Data Collection

This study utilised both qualitative and quantitative data. The qualitative component involved a systematic literature review and a meta-analysis to integrate results from various scientific studies [30]. The quantitative aspect involves the objective evaluation, synthesis, and summarisation of findings using descriptive statistics. These statistics provide a numerical summary of the data, helping to identify patterns, trends, and relationships within the data set. In this research, we carefully selected journal publications by looking for ones that had precise research methods, suitable sampling procedures, relevance of the analysis, and data validity. Table 2 is the tool used to organise and filter data for analysis which include authors details, publication year, paper quality where impact factor was considered, Approach which could be qualitative, quantitative or mixed, Sampling how papers were selected , Analysis implies techniques used for analysing the data, such as statistical analysis or thematic coding., validity which defines the correctness of the findings in a paper and the discussed impacts of blockchain on data security and privacy.

### 3.4 Data Analysis

In this research, we primarily employed descriptive statistics, focusing on frequencies and percentages, to analyse the collected data. The data was initially gathered and organised using a statistical package spreadsheet before undergoing analysis. To ensure the study's reliability, we utilised a quality criteria checklist developed by [31] to categorise factors, as Table 2: Data Capture Worksheet outlined. These categories were substantiated by credible sources [32,33]. Additionally,

we implemented the paper sorting criteria described earlier to guarantee the accuracy of the data. A collaborative review of articles that met the specifications was conducted to uphold the study's quality. Moreover, it followed guidance provided by [34] on the importance of data cleaning before analysis to ensure the precision of our findings.

Table 1: Sources of publications

| Publication Source | Frequency |
|---|---|
| International Journal of Innovative Research in Science, Engineering and Technology | 1 |
| IEEE Access | 1 |
| INTERNATIONAL CONFERENCE ON EURASIAN ECONOMIES 2019 | 1 |
| Blockchain Frontier Technology (B-Front) | 1 |
| AIS Electronic Library (AISeL) | 1 |
| Transportation Research | 4 |
| ICONNECT | 2 |
| International Journal of Production Research | 1 |
| International Research Journal of Modernization in Engineering Technology and Science | 1 |
| University of Nebraska – Lincoln | 1 |
| Istanbul Business Research | 1 |
| Academy of Accounting and Financial Studies Journal | 1 |
| IRJET | 1 |
| Journal of Emerging Technologies and Innovative Research | 1 |
| National Institute of Standards and Technology | 1 |
| Journal of Computational Innovations and Engineering Applications 5(2) 2021: 8–14 | 1 |
| International Journal of Creative Research Thoughts | 1 |
| Business & Information Systems Engineering | 2 |
| Financial Innovations | 1 |
| International Journal of Information Systems and Project Management | 1 |
| International Conference on Blockchain Technology and Applications (ICBTA) | 1 |
| Egyptian Informatics Journal | 1 |
| Measurement: Sensors | 3 |
| Internet of Things and Cyber-Physical Systems | 1 |
| Future Internet | 1 |
| IJRAR- International Journal of Research and Analytical Reviews | 9 |
| Advances in Social Science, Education, and Humanities Research | 1 |
| International Journal of Health Sciences and Pharmacy (IJHSP) | 1 |
| IOP Conference Series: Earth and Environmental Science | 1 |
| 2017 IEEE 6th International Congress on Big Data | 1 |
| Total | 45 |

### 3.5 Findings and Discussion

The study's findings were meticulously outlined and deliberated, offering valuable perspectives on the potential effect of blockchain technology on data security and privacy within the ICT industry. Through a comprehensive review of existing literature and analysis of real-world data, the researchers thoroughly evaluated the influence of blockchain technology, allowing them to address the study's objectives effectively.

### 3.6 Ethical Considerations

The research was meticulously conducted, with a strong focus on ethical principles to protect the privacy and confidentiality of the gathered information. It strictly followed established ethical guidelines and protocols. Through this approach, the study sought to thoroughly examine the effects of blockchain technology on data security and privacy to advance knowledge in the field and guide the development of real-world solutions that bolster data protection.

Table 2: Data capture worksheet

| Authors | Year | Paper quality | Approach | Sampling | Analysis | Validity | Impact of Block Chain on Data Security and Privacy | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | F1 | F2 | F3 | F4 |
| | | | | | | | □ | □ | □ | □ |

F1 - Enhanced Data Security
F2 - Improved Data Privacy
F3 - Use Cases in Data Security
F4 - Trustworthiness and Transparency

## 4. RESULTS AND DISCUSSION

There has been a significant amount of research on the wide-ranging advantages of blockchain technology. This study aims to organise these benefits into two main categories: the global impact and the impact on a local level, with a specific focus on Tanzania. The research is particularly crucial due to the lack of existing literature on how blockchain influences data security and privacy in Tanzania. The upcoming sections will delve into this classification in detail. Additionally, Table 3 summarises the papers by indicating year of publication, number of occurrences and the corresponding percentage. In contrast, Table 4 offers more insight of all the documents used to assess the impact of blockchain on information security by displaying the merits along with number of occurrences in publications.

Table 3: Research papers counts published from 2016 to 2023

| Year | Frequency | Percentage |
|---|---|---|
| 2016 | 0 | 0.00 |
| 2017 | 4 | 8.89 |
| 2018 | 9 | 20.00 |
| 2019 | 8 | 17.78 |
| 2020 | 7 | 15.56 |
| 2021 | 5 | 11.11 |
| 2022 | 6 | 13.33 |
| 2023 | 6 | 13.33 |
| **Total** | **45** | **100** |

Table 3 shows that most academic papers were released from 2016 to 2023, during which a noticeable surge in significant cyberattacks had a far-reaching impact on global information systems. Several high-profile security breaches marked this period. 2016, for instance, a staggering 6.5 million passcodes from LinkedIn were illicitly obtained [35]. Similarly, around the same time, approximately 136 million user accounts from MySpace were offered for sale on the Dark Web. Another noteworthy incident was the revelation by Yahoo of a data breach where 1billion user accounts information were accessed a hacking group by December 2016 [36]. Moreover, according to [37], there were substantial repercussions for various U.S. government agencies and private enterprises, while [38] reported that a company paid a ransom of approximately $4.4 million to the attackers. Although specific data on the impact of these incidents on businesses in Africa and Tanzania during this timeframe is not readily available, overall statistics indicate a general escalation in cybersecurity threats. This underscores the pressing need for a robust, comprehensive approach to safeguarding data and privacy.

### 4.1 Impact of Blockchain Technology in Securing Information Systems: Global Context

In this section of the study, a comprehensive review was conducted, analysing a total of 45 original research papers from diverse geographical locations within the field of information security. These papers, spanning 2016 to 2023 and meeting rigorous quality standards, delve deep into the exploration of blockchain technology and its pivotal role in fortifying information systems. Through meticulous analysis, the papers shed light on the intricate challenges in the global ICT sector, particularly about implementing blockchain, with a specific emphasis on data security and privacy concerns. The findings are summarised in a detailed table, providing a comprehensive overview of the prevalent everyday challenges associated with integrating blockchain in information systems worldwide.

The study findings suggest that blockchain technology significantly enhances global data security, privacy, and trust. These findings are extrapolated to anticipate potential implications for the Tanzanian context. More literature is needed to support the use of blockchain in Tanzania for data security. The comprehensive literature review has yielded crucial insights, which will be elaborated on in the subsequent sections.

Table 4: Impact of blockchain technology on security and privacy: Global context

| Merits listed in particular Publication | Frequency | | | Percentage | | |
|---|---|---|---|---|---|---|
| | YES | NO | TOTAL | YES | NO | TOTAL |
| **Enhanced Data Security** | **37** | **8** | **45** | **82.2%** | **17.8%** | **100%** |
| **Improved Data Privacy** | **32** | **13** | **45** | **71.1%** | **28.9%** | **100%** |
| **Use Cases in Data Security** | **34** | **11** | **45** | **75.6%** | **24.4%** | **100%** |
| **Trustworthiness and Transparency** | **36** | **9** | **45** | **80.0%** | **20.0%** | **100%** |

1. **Enhanced data security:** The research findings indicate that a significant majority, precisely 82.2% of the literature, emphasises the efficacy of blockchain technology in safeguarding data within the ICT industry. This aligns with the reference [39], which underscores blockchain's decentralised nature as a robust defence mechanism against unauthorised alterations and tampering, consequently leading to a substantial decrease in the likelihood of data breaches.
2. **Enhanced data privacy:** Blockchain technology has been widely recognised for enhancing data privacy, with 71.1% of the literature confirming its positive impact. As discussed by [40], blockchain technology's consensus processes and encryption algorithms are pivotal in strengthening data privacy. One of the key components contributing to this is public-private key cryptography, which empowers users to have control over data sharing and ensures secure data transmission and authentication. The transparency offered by blockchain technology also allows users to effectively manage how their data is shared, thereby safeguarding sensitive information from unauthorised disclosure.
3. **Trustworthiness and transparency:** The literature extensively demonstrates that blockchain significantly impacts transparency and trust, gaining support from 75.5% of the sources. Blockchain technology's consensus processes and transparency mechanisms are crucial in creating more dependable ICT systems. As emphasised in citation [41], the decentralised architecture of blockchain technology plays a pivotal role in mitigating the vulnerabilities associated with single points of failure and eliminates the need for centralised authorities. This trustless and distributed model enables participants to independently validate data transactions, thereby enhancing transparency, enforcing accountability, and markedly diminishing the likelihood of unauthorised alterations to the data.
4. **Use cases for blockchain technology in data security:** According to 80% of the literature, blockchain technology has been shown to significantly enhance data security and privacy across a wide range of applications. This includes its use in IoT networks and healthcare systems, where blockchain technology is crucial in ensuring data integrity, secure device connections, and safe patient data storage and exchange. Notably, a specific study [16] highlights the importance of blockchain in maintaining data integrity and securing device connections in healthcare settings, highlighting its potential to revolutionise data security in healthcare.

### 4.2 Role Played by Blockchain Technology in Securing Information Systems in Tanzania

There has yet to be any known use of blockchain technology for securing information systems in Tanzania. The country faces persistent challenges with data management across various sectors, including e-commerce, media, agriculture, land administration, and natural resources [11,12]. Moreover, infrastructure, manufacturing, retail, services, and healthcare sectors also encounter hurdles [13]. In contrast to countries like Ghana, Ethiopia, and Kenya, which have effectively implemented blockchain technology, Tanzania needs to catch up. For instance, Kenya has employed blockchain for micro-lending to farmers [42], Ghana has facilitated property registration for over 80% of landowners, and Ethiopia has monitored coffee exports to verify the origin and chemical exposure of the coffee.

In Tanzania, the implementation of blockchain technology in the healthcare sector has the potential to improve the security and management of patient records significantly. Currently, many hospitals in Tanzania are grappling with severe security issues related to patient records, including unauthorised access that compromises patient privacy and confidentiality. This unauthorised access raises the risk of identity theft and manipulation of sensitive medical data. Moreover, the ineffective transfer of patient records between hospitals results in redundancy in medical tests and escalating costs for both patients and hospitals. The presence of inaccurate data and underutilisation of bandwidth further exacerbates these challenges [42].

In Tanzania, the land registration sector faces significant challenges, such as bureaucratic inefficiencies, corruption, and a lack of transparency [43]. These issues have hampered the country's land registration process. The government's attempt to address these problems by deploying the Integrated Land Management Information System has been plagued by persistent data security and storage issues, leading to a time-consuming registration process [43]. However, the potential of blockchain for individuals and organisations is promising. Using blockchain, Tanzania could streamline the land registration process, enhance data security, and prevent unauthorised alterations to registered information. This can significantly improve transparency and authentication of land ownership in the country.

The banking sector faces significant challenges, including frequent network outages, unauthorised fund transfers, delays in fund delivery, and difficulties in transaction reconciliation. These issues have adversely affected the efficiency and security of mobile banking [44]. Additionally, the industry is confronted with issues related to fraudulent activities and insufficient internal controls, which seriously threaten the integrity of banking operations [45]. Similarly, educational institutions are grappling with the limitations of their current systems for managing and safeguarding student records, consequently making them vulnerable to instances of degree fraud. Implementing blockchain is believed to be a profound solution to address these complex issues. Organisations can achieve secure, transparent, and reliable data storage by leveraging blockchain, potentially mitigating banking and education problems.

## 5. CONCLUSIONS

According to sources, blockchain technology in Tanzania could provide substantial advantages across various sectors, such as healthcare, banking, education, and land registration. The inherent features of blockchain, including robust security measures, enhanced anonymity, increased data confidentiality, and improved transparency, have the potential to effectively address the prevalent challenges related to data storage and management in these industries. Embracing blockchain technology has the potential to bolster data security measures, mitigate instances of fraud, and streamline operational processes, thereby reducing the expenses associated with traditional methodologies.

The results of this research provide crucial and valuable insights for a wide range of stakeholders, including professionals, policymakers, and researchers. The study underscores the importance and potential benefits of integrating blockchain technology into various sectors in Tanzania. It suggests that professionals can benefit from examining successful blockchain implementation models in countries like Ghana and Kenya and applying similar practices in Tanzania. Policymakers are urged to focus on creating a conducive environment that promotes the adoption of blockchain technology. Additionally, the research highlights the importance of further exploring Tanzania's blockchain landscape, particularly in law, business, healthcare, and education. Given Tanzania's early-stage adoption of blockchain, it emphasises the need for in-depth sector-specific studies and comparisons with well-established blockchain ecosystems, which can provide valuable insights for a smooth integration of blockchain technology within Tanzania and on a global scale.

## REFERENCES

[1] Wang, H. (2022). Big Data Security Management Countermeasures in the Prevention and Control of Computer Network Crime. Journal of Global Information Management (JGIM), 30(7), 1-16. http://doi.org/10.4018/JGIM.295450.

[2] Mwemezi, J., & Mandari, H. (2024). Big data analytics usage in the banking industry in Tanzania: does perceived risk play a moderating role on the technological factors, Journal of Electronic Business & Digital Economics, Emerald Group Publishing Limited, 3(3),318-340. doi: 10.1108/JEBDE-01-2024-0001.

[3] Bertino, E. (2014). Data Security – Challenges and Research Opportunities. In Proceedings of the Conference Title, 9-13. http://dx.doi.org/10.1007/978-3-319-06811-4_2.

[4] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Online, https://assets.pubpub.org/d8wct41f/31611263538139.pdf, Retrieved June 26, 2024.

[5] Mohsin, A., Zaidan, A., Bahaa, B., Albahri, O. S., Albahri, A. S., Alsalem, M. A., & Mohammed, K. (2019). Blockchain-PSO-AES Techniques in Finger Vein Biometrics: A Novel Verification Secure Framework for Patient Authentication. Computer Standards & Interfaces, 66(1), 103-111. https://doi.org/10.1016/j.csi.2019.04.002.

[6] Wang, H., Smagghe, G., & Meeus, I. (2018). The Single von Willebrand factor C-domain protein (SVC) coding gene is not involved in the hymenopteran upregulation after Israeli acute paralysis virus (IAPV) injection in the bumblebee Bombus terrestris. Developmental and comparative immunology, 81, 152–155. https://doi.org/10.1016/j.dci.2017.11.011.

[7] Chen, L., Lee, W. K., Chang, C.-H., Choo, K.-K. R., & Zhang, N. (2019). Blockchain-based searchable encryption for electronic health record sharing. Future Generation Computer Systems, 95(1), 50-60. https://doi.org/10.1016/j.future.2019.01.018.

[8] Cao, S., Zhang, G., Liu, P., Zhang, X., & Neri, F. (2019). Cloud-Assisted Secure eHealth Systems for Tamper-Proofing EHR via Blockchain. Information Sciences, 485. 427-440. https://doi.org/10.1016/j.ins.2019.02.038.

[9] Islam, M. R., Rahman, M. M., Mahmud, M., Rahman, M. A., Mohamad, M. H. S., & Embong, A. H. (2021). A review on blockchain security issues and challenges. Proceedings of the 2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC), 227-232. Shah Alam, Malaysia. http://dx.doi.org/10.1109/ICSGRC53186.2021.9515276.

[10] Moosavi, N., & Taherdoost, H. (2023). Blockchain technology application in security: A systematic review. *Blockchains*, 1(2), 58-72. https://doi.org/10.3390/blockchains1020005.

[11] Nkwabi, J. (2021). A Review of the Significance of Blockchain Technology in Tanzania. European Journal of Business and Management, 13(16), 1-5. https://doi.org/10.7176/EJBM/13-16-01.

[12] Maagi, B. (2023). Applicability of blockchain technology in improving efficiency in supply chain operations in public procurement in Tanzania. International Journal of Research in Business and Social Science, 12(9), 91-98. https://doi.org/10.20525/ijrbs.v12i9.2995

[13] Canellis, D. (2018). Tanzania: The government is researching blockchain tech, but it is doing so very slowly. Hard Fork The Next Web, https://thenextweb.com/news/tanzania-blockchain-research, Retrieved October 26, 2024.

[14] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc. 124-152.
[15] Saah, A. E. N., Yee, J.-J., & Choi, J.-H. (2023). Securing construction workers' data security and privacy with blockchain technology. Applied Sciences, *13*(24), 13339. https://doi.org/10.3390/app132413339.
[16] Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352. https://doi.org/10.1504/IJWGS.2018.095647.
[17] Yu, H. G. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 3(2),100067. https://doi.org/10.1016/j.bcra.2022.100067.
[18] Elisa, N., Yang, L., Chao, F., & et al. (2023). A framework of blockchain-based secure and privacy-preserving e-government system. *Wireless Networks, 29*, 1005–1015. https://doi.org/10.1007/s11276-018-1883-0.
[19]. Ferrag, M. A., & Shu, L. (2021). The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. *IEEE Internet of Things Journal, 8*(24), 17236-17260. https://doi.org/10.1109/JIOT.2021.3078072.
[20] Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE International Congress on Big Data, 557-564. https://doi.org/10.1109/BigDataCongress.2017.85.
[21] Zhang, R., Xue, R., Liu, L. (2019). Security and Privacy on Blockchain. *ACM Digital Library*, 52(3), 1-34 https://doi.org/10.1145/3316481.
[22] Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 34, 11475–11490. https://doi.org/10.1007/s00521-020-05519-w.
[23] Dwivedi, A.D., Srivastava, G., Dhar, S., & Singh, R. (2019). A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors, 19(2), 326. https://doi.org/10.3390/s19020326.
[24] Choudhury, P., & Kumar, N. (2020). Blockchain-based secure communication for Internet of Things: A systematic review. Journal of Network and Computer Applications, 154, 102602.
[25] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, Data Privacy and Blockchain: a review. SN Computer Science Computer Science, 3,127. https://doi.org/10.1007/s42979-022-01020-4.
[26] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 243-252. https://doi.org/10.1109/ICSA.2017.33.
[27] Reegu, F., Abas, H., Hakami, Z., Tiwari, S., Dziyauddin, R., Muda, I., Almashaqbeh, H., & Jain, R. (2022). Systematic Assessment of the Interoperability Requirements and Challenges of Secure Blockchain-Based Electronic Health Records. Security and Communication Networks, 2022, 1-12. https://doi.org/10.1155/2022/1953723.
[28] Balasubramanian, S., Sethi, J., Ajayan, S., & Paris, C. (2022). An enabling framework for Blockchain in Tourism. Information Technology & Tourism, 24, 165-179. https://doi.org/10.1007/s40558-022-00229-6.
[29] Valeri, M., Baggio, R. (2020). A critical reflection on the adoption of blockchain in tourism. Information Technology & Tourism, 23, 121–132. https://doi.org/10.1007/s40558-020-00183-1.
[30] Deckers, R., & Lago, P. (2022). Systematic literature review of domain-oriented specification techniques. Journal of Systems and Software, 192, 1-11. https://doi.org/10.1016/j.jss.2022.111415.
[31] Hassan, N. H., Ismail, Z., & Maarop, N. (2015). Information security culture: A systematic literature review. Proceedings of the International Conference on Cybersecurity (ICOCI), Istanbul, Turkey, 11-13. https://api.semanticscholar.org/CorpusID:156010250.
[32] Arbanas, K., & Hrustek, N. Ž. (2019). Key success factors of information systems security. Journal of Information and Organizational Sciences, 43(2), 131-144. https://doi.org/10.31341/jios.43.2.1.
[33] Bolek, V., Látečková, A., Romanová, A., & Korcek, F. (2016). Factors affecting information security focused on SME and agricultural enterprises. Agris On-line Papers in Economics and Informatics, 8(4), 37-50. http://dx.doi.org/10.22004/ag.econ.253226.
[34] Ridzuan, F., & Zainon, W. M. (2019). A Review of data cleansing methods for big data. The Fifth Information Systems International Conference, Procedia Computer Science, 161, 731-738. https://doi.org/10.1016/j.procs.2019.11.177.
[35]Pagliery, J. (2016). Hackers are selling 117 million LinkedIn passwords. CNNMoney. Retrieved May 15, 2024, from fhttps://money.cnn.com/2016/05/19/technology/linkedin-hack/index.html.
[36] Hill, M.,Swinhoe, D., & Leyden,J. (2024). The biggest data breaches of the 21st century. CSO United States., from https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html, Retrieved October 26, 2024.
[37] U.S. Government Accountability Office. (2020). Federal Response to Cybersecurity Incidents: Lessons Learned from the SolarWinds and Microsoft Exchange Attacks. GAO-22-104746, https://www.gao.gov/products/gao-22-104746, Retrieved June 10, 2024.

[38] CISA. (2021). "Attack on Colonial Pipeline: What We've Learned and What We've Done Over the Past Two Years. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-whatweve-learned-what-weve-done-over-past-two-years, Retrieved May 10, 2024.
[39] Kosba, A. E., Miller, A. K., Shi, E., Wen, Z. A., & Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. IEEE Symposium on Security and Privacy (SP), San Jose, CA, 839-858. doi: 10.1109/SP.2016.55.
[40] Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero-knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. Journal of Information Security and Applications, 80, 103678. https://doi.org/10.1016/j.jisa.2023.103678.
[41] Mougayar, W. M. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. John Wiley & Sons, Inc.
[42] Kombe, C., Sam, A., Ally, M., & Finne, A. (2019). Blockchain Technology in Sub-Saharan Africa: Where does it fit in Healthcare Systems: A case of Tanzania. Journal of Health Informatics in Developing Countries, 13(2), 1-19.
[43] Kombe, M., Manyilizu, D., & Mvuma, P. (2017). Design of Land Administration and Title Registration Model Based on Blockchain Technology. Journal of Information Engineering and Applications, 7 (1), 8-15.
[44] Ulrich-Diener, F., Dvouletý, O., & Špaček, M. (2023). The future of banking: What are the actual barriers to bank digitalisation?. Business Research Quarterly, 26(3), 234-244. https://doi.org/10.1177/23409444231211597.
[45] Jelodar, M. (2016). Prioritisation of the Factors Affecting Bank Efficiency Using Combined Data Envelopment Analysis and Analytical Hierarchy Process Methods. Journal of Optimization, 1-7. https://doi.org/10.1155/2016/5259817.