Original Article

Blockchain Resilience and Public Service Delivery: Empirical Evidence from Kenya's National Government Ministries

Moses Kibet Yegon Ngetich[1], Dr. Alfred K. Bett, PhD[1] & Dr. Tom Alex Obulemire, PhD[1]*

[1] University of Kabianga, P. O. Box 2030-20200, Kericho, Kenya.
* Author's ORCID ID; https://orcid.org/0009-0003-5944-5696; Email: moseskibett@gmail.com

ABSTRACT

As governments increasingly adopt emerging technologies to improve public service delivery, blockchain has gained prominence for its unique attributes, including resilience. Resilience, in the context of blockchain, refers to the system's ability to maintain functionality despite faults, disruptions, or cyber threats, making it especially relevant for sustaining uninterrupted service in critical government operations. This study examines the relationship between blockchain technology resilience and service delivery in Kenya's national government ministries. Anchored in the New Public Management (NPM) theoretical framework, the study employed a cross-sectional survey involving 319 respondents: 220 government officials and 99 citizens, selected through stratified and purposive sampling. Data were collected using structured questionnaires and analysed through multiple regression analysis. The results revealed a statistically significant and positive relationship between blockchain resilience and service delivery ($\beta = 0.287$, $p < 0.05$), suggesting that robust and fault-tolerant blockchain systems can enhance efficiency, continuity, and public confidence in service delivery. The study recommends that government institutions prioritise the integration of resilient digital infrastructure to strengthen service delivery outcomes.

INTRODUCTION

The delivery of timely, efficient, and reliable public services is a critical mandate for governments worldwide. In the context of developing countries such as Kenya, national government ministries face persistent challenges, including bureaucratic delays, frequent system failures, and low citizen trust in government processes (World Bank, 2017; OECD, 2018). These inefficiencies have led to a growing demand for technology-driven reforms aimed at enhancing service performance, transparency, and accountability (Smith & Johnson, 2019). Among the emerging technologies gaining global attention is blockchain, a decentralised, tamper-proof, and distributed ledger system initially developed for cryptocurrency but now increasingly applied across various sectors, including governance (Gupta & Bansal, 2020). While much of the discourse around blockchain in public administration has focused on its immutability and transparency, another essential but underexplored attribute is resilience. Blockchain resilience refers to the system's ability to maintain functionality under conditions of stress, such as hardware failure, cyberattacks, or operational disruptions (Zhang et al., 2019; Baguinda et al., 2021). This attribute is of particular importance in government settings, where service continuity is vital to uphold citizen trust and ensure access to essential services (Rodriguez & Scholl, 2018).

In a governance environment often constrained by fragile digital systems and fragmented data infrastructure, blockchain resilience can offer a transformative solution (Laurent & Moreau, 2018). Through features such as distributed nodes, consensus mechanisms, and cryptographic security, blockchain ensures that services are not interrupted even when parts of the system are compromised. This ability to provide fault tolerance and operational continuity makes blockchain resilience especially relevant for national government ministries in Kenya, where digital transformation is ongoing and systemic weaknesses still pose a threat to service reliability (Ofori & Mensah, 2020). This study seeks to empirically assess the relationship between blockchain technology resilience and service delivery in Kenya's national government ministries. While several studies have highlighted the potential of blockchain to improve public services, there remains a significant research gap in understanding how resilience specifically contributes to service delivery outcomes (Van Der Merwe, 2023). This paper addresses that gap by evaluating how the robustness and reliability of blockchain systems influence key dimensions of service delivery, such as efficiency, accessibility, and responsiveness. The study is anchored in the New Public Management (NPM) theoretical framework, which emphasises efficiency, performance measurement, and the adoption of private-sector–style innovations to improve public sector operations (Hood, 1991; Dunleavy & Hood, 1994). NPM supports the integration of resilient technologies that ensure continuous service provision, reduce system downtime, and enhance citizen satisfaction.

LITERATURE REVIEW

The New Public Management (NPM) framework emerged in the 1980s as a shift in public administration thought, promoting efficiency, responsiveness, and customer-centric services in the public sector (Hood, 1991). It encourages the

adoption of private-sector tools, including digital innovations, to achieve performance-oriented governance (Christensen & Lægreid, 2007; Dunleavy & Hood, 1994). In this context, blockchain resilience aligns with NPM by enhancing the robustness of public systems, ensuring that service delivery continues even in the face of disruptions.

Blockchain's fault-tolerant design and distributed control exemplify NPM's emphasis on reducing systemic fragility and improving service efficiency. Initially developed for cryptocurrency transactions, blockchain technology has since found relevance in public sector applications such as identity verification, procurement, records management, and digital voting (Gupta & Bansal, 2020; Nakamoto, 2008). Governments globally are increasingly leveraging blockchain to improve trust, data integrity, and operational efficiency (Rodriguez & Scholl, 2018).

Blockchain resilience refers to the system's ability to recover from and resist failure (Zhang et al., 2019; Baguinda et al., 2021). This resilience is achieved through distributed nodes, cryptographic integrity, and consensus protocols that eliminate single points of failure (Park et al., 2020; Laurent & Moreau, 2018). In fragile public ICT environments such as those common in developing countries, resilience ensures service uptime, continuity, and confidence in system integrity (Ofori & Mensah, 2020).

Effective service delivery comprises dimensions such as timeliness, accessibility, responsiveness, and fairness (World Bank, 2017; OECD, 2018). In Kenya, national ministries are central to public service management, yet they suffer from legacy systems, technical failures, and bureaucratic inefficiencies, issues that resilience-oriented technologies seek to address (Smith & Johnson, 2019). By reducing downtime, preserving data, and supporting seamless operations, blockchain resilience can significantly enhance citizen trust and institutional credibility (Wang & Li, 2019; Laurent & Moreau, 2018).

While prior studies have explored blockchain transparency and immutability extensively, few have isolated resilience as a standalone factor influencing service quality (Van Der Merwe, 2023). Most existing literature either subsumes resilience under broader technological attributes or fails to empirically examine its specific contribution to service delivery outcomes. Furthermore, much of the existing research has focused on advanced economies, where digital infrastructure is mature and service interruptions are less frequent.

This study addresses these gaps by isolating blockchain resilience as a distinct analytical construct and empirically assessing its influence on service delivery within Kenya's national government ministries. By doing so, it extends the NPM framework by showing how resilience, characterised by fault tolerance, system uptime, and decentralised architecture, can enhance performance, efficiency, and user satisfaction in the public sector. This contribution is especially relevant for developing contexts where system fragility and operational disruptions frequently undermine digital service effectiveness.

METHODOLOGY

This study employed a quantitative research approach using a cross-sectional survey design. This design was selected for its ability to collect data from a wide range of respondents at a single point in time, facilitating the assessment of prevailing perceptions and testing of relationships between blockchain resilience and public service delivery (Christensen & Lægreid, 2007). Quantitative analysis was appropriate given the study's goal of statistically examining associations between variables and drawing generalizable conclusions based on empirical evidence.

The target population for the study consisted of two distinct groups: government officers working in national government ministries headquartered in

Nairobi County, and citizens who had recently accessed services from these ministries. Government officers were selected based on their involvement in service planning, implementation, and monitoring, while citizens were included to provide first-hand experiential feedback on the quality, accessibility, and responsiveness of public services (OECD, 2018).

To ensure representativeness and depth, a combination of stratified and purposive sampling techniques was employed. Stratification enabled balanced sampling across ministries and between the two respondent categories, staff and citizens, while purposive sampling allowed for the intentional selection of individuals with relevant knowledge and experiences regarding the services under investigation. A total of 319 respondents participated in the study, comprising 220 government officers and 99 citizens. The sample size was calculated using Yamane's formula, which supports statistically valid estimates for finite populations within acceptable margins of error (Yamane, 1967).

Data for the study were collected using a structured questionnaire consisting of two main sections. Section A captured demographic and institutional information, while Section B focused on key constructs, namely blockchain resilience and service delivery, measured using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). The questionnaire items were developed based on validated constructs drawn from existing literature (Baguinda et al., 2021; Wang & Li, 2019) and were then adapted to reflect the specific context of the Kenyan public sector.

To ensure instrument quality, a pilot test was conducted with a small group of respondents to evaluate the clarity, reliability, and validity of the items. Feedback from the pilot exercise informed minor revisions to the tool prior to full deployment. To assess internal consistency, Cronbach's alpha was calculated for all subscales, with each exceeding the acceptable threshold of 0.7, thus confirming the instrument's reliability.

Ethical clearance for this study was obtained from the University of Kabianga's Research and Ethics Committee. Participation was voluntary, and all respondents provided informed consent before taking part in the study. Respondent anonymity and confidentiality were strictly maintained, and all data collected were used solely for academic purposes.

The collected data were coded and analysed using SPSS. The analysis process involved several key steps. First, descriptive statistics were computed to summarise demographic characteristics and assess central tendencies across the main constructs. Next, reliability testing was performed using Cronbach's alpha to confirm the internal consistency of the measurement scales. Finally, a simple linear regression analysis was conducted to examine the relationship between blockchain resilience and service delivery. The hypothesis was tested at a significance level of 0.05, with interpretation focused on the standardised beta coefficient (β) to assess the strength of the relationship, and the coefficient of determination (R^2) to evaluate the explanatory power of the model.

FINDINGS AND DISCUSSIONS

Descriptive statistics were computed to summarise perceptions of blockchain resilience and service delivery across the two respondent categories: government officers and citizens. The results are presented in Table 1.

Table 1: Descriptive Statistics for Key Constructs

Construct	Group	Mean	SD
Blockchain Resilience	Government Officers	3.71	0.56
Blockchain Resilience	Citizens	3.59	0.63
Service Delivery	Government Officers	3.84	0.51
Service Delivery	Citizens	3.78	0.56

These results show a generally positive perception across both groups. Among government officers, the mean score for blockchain resilience was 3.71 (SD = 0.56), reflecting strong agreement that systems within national ministries exhibit resilience attributes, such as continuity during system faults, tolerance to cyber threats, and minimal downtime. This aligns with observations of improved transaction consistency in functions such as procurement, payroll, and licensing (Laurent & Moreau, 2018).

Citizen respondents reported a slightly lower resilience mean of 3.59 (SD = 0.63), reflecting cautious optimism regarding digital platform reliability. Sporadic service delays were mentioned, suggesting uneven rollout of blockchain-backed solutions. Still, responses were largely favourable in areas such as civil registration and online applications (Rodriguez & Scholl, 2018).

For service delivery, government officers recorded a mean of 3.84 (SD = 0.51), and citizens 3.78 (SD = 0.56), reflecting moderately high satisfaction with timeliness, accessibility, and efficiency. This perception was consistent with increasing system stability and predictability (World Bank, 2017; Smith & Johnson, 2019).

To evaluate the relationship between blockchain resilience and service delivery, a simple linear regression analysis was conducted. Table 2 presents the regression results.

Table 2: Linear Regression Output

Predictor	β	R²	p-value
Blockchain Resilience	0.287	0.501	< 0.05

The regression coefficient ($\beta = 0.287$) indicates a positive and moderately strong effect of blockchain resilience on service delivery. With $R^2 = 0.501$, about 50.1% of the variation in service delivery can be explained by blockchain resilience, and the p-value confirms the relationship is statistically significant.

These findings validate the hypothesis that resilience, through system redundancy, uptime, and fault tolerance, enhances public service delivery. From an NPM perspective, this supports the argument for performance-oriented, technology-driven public systems (Hood, 1991; Dunleavy & Hood, 1994).

The results are consistent with Park et al. (2020), who found that blockchain-based systems in the UK improved service reliability. Similarly, Wang & Li (2019) documented how decentralised architectures enhance system continuity during failures. However, unlike these developed contexts, this study is situated in a lower-resource setting, highlighting the relevance of resilience where systemic vulnerabilities are more common. It also diverges from earlier studies that treated resilience as a secondary feature, instead establishing it as a central driver of public service quality.

The slight divergence in perceptions between officers and citizens may stem from familiarity gaps. Officers, being directly involved with systems, are likely to appreciate back-end improvements. Citizens, however, base their judgments on front-end usability, which may suffer from inconsistencies in rollout and support. This underscores the need for inclusive resilience planning, balancing infrastructure robustness with user-facing design and accessibility (Ofori & Mensah, 2020; Van Der Merwe, 2023).

This study contributes to the literature by empirically isolating blockchain resilience, distinct from the more explored traits of transparency and immutability (Zhang et al., 2019; Abiteboul & Stoyanovich, 2019). In Kenya's context, where ministries depend heavily on automated platforms for payroll, licensing, and procurement, ensuring resilience is critical. Downtime can delay salaries, disrupt essential services, and erode public trust,

particularly in politically sensitive or high-demand sectors.

Finally, these findings reinforce the need for government institutions to embed resilience metrics (e.g., system availability, failure recovery time) into their digital transformation scorecards. While initial automation efforts are common, few institutions invest in stress testing or failover planning, leaving services vulnerable during crises. As such, resilience must not be viewed as a luxury but as a strategic imperative for reliable and citizen-centred service delivery in digital governance.

CONCLUSION AND RECOMMENDATION

Conclusion

This study set out to assess the relationship between blockchain technology resilience and service delivery in Kenya's national government ministries. Drawing on the New Public Management (NPM) framework and empirical data from both government officers and citizens, the study established a statistically significant and positive relationship between the resilience of blockchain systems and the quality of public services delivered. With a regression coefficient of $\beta = 0.287$ and $p < 0.05$, the results demonstrate that resilient blockchain infrastructure plays a pivotal role in ensuring efficiency, continuity, and public confidence in government service delivery.

From a theoretical perspective, the findings extend the application of NPM by demonstrating that resilience, though often regarded as a technical attribute, can be interpreted as a governance enabler. Resilient systems support the core objectives of NPM; performance, responsiveness, and citizen-centred service delivery by enabling ministries to maintain functionality in the face of cyber threats, system failures, or data loss (Hood, 1991; Dunleavy & Hood, 1994).

From a practical standpoint, the study highlights the importance of prioritising resilience in the design and implementation of digital infrastructure. As

government institutions in Kenya and other developing contexts continue to digitise, they must move beyond superficial automation efforts and invest in robust, distributed, and fault-tolerant systems that can operate consistently under pressure (Zhang et al., 2019; Park et al., 2020).

However, this study is not without limitations. Its cross-sectional design limits the ability to establish causality, and its focus on ministries headquartered in Nairobi may limit generalizability to other government tiers or regions. Future studies could employ longitudinal or comparative designs to build on these findings.

Recommendation

Based on the study's findings, particularly the strong association between blockchain resilience and service delivery performance, several actionable recommendations are proposed:

- **Embed resilience into system design:** Ministries should adopt blockchain-based platforms with built-in fault tolerance, redundancy, and decentralisation. This aligns with the study's finding that 50.1% of the variation in service delivery is explained by system resilience.

- **Invest in infrastructure stress testing and performance audits:** Regular simulations and recovery drills will identify system vulnerabilities before actual failures occur (Laurent & Moreau, 2018). This is critical given the observed sensitivity of service delivery to resilience gaps.

- **Build capacity in resilience engineering:** ICT staff should undergo continuous training on blockchain management, system hardening, and incident response. The study revealed that system performance perception varied between internal staff and citizens, indicating that internal readiness is key.

- **Track resilience indicators within performance frameworks:** Metrics such as system uptime, incident response time, and service recovery duration should be institutionalised to ensure resilience is not only designed but also monitored.

- **Promote inclusive user-centred resilience planning:** Given the perceptual differences between staff and citizens, design efforts should balance backend security with frontend usability, ensuring continuity is visible to all service users.

In conclusion, blockchain resilience should be seen not merely as a technical feature but as a strategic driver of effective, responsive, and trustworthy digital governance. Its integration into national digital systems is essential for sustaining public confidence and ensuring uninterrupted access to services, especially in fragile governance contexts.

AREA FOR FURTHER RESEARCH

Future research should explore mediating and moderating variables that influence the relationship between blockchain resilience and service delivery. Variables such as digital literacy, institutional trust, and user participation may shape outcomes. In-depth studies using longitudinal or comparative designs across various government levels would offer richer insights and strengthen the generalizability of findings.

REFERENCES

Abiteboul, S., & Stoyanovich, J. (2019). Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation. *Journal of Data and Information Quality, 11*(1), 1–9. https://doi.org/10.1145/3316411

Baguinda, M., Thapa, D., & Adhikari, C. (2021). Blockchain resilience in healthcare systems: A Nepalese perspective. *Government Information Quarterly, 38*(2), 101573. https://doi.org/10.1016/j.giq.2021.101573

Christensen, T., & Lægreid, P. (2007). The whole-of-government approach to public sector reform. *Public Administration Review, 67*(6), 1059–1066. https://doi.org/10.1111/j.1540-6210.2007.00797.x

Dunleavy, P., & Hood, C. (1994). From old public administration to new public management. *Public Money & Management, 14*(3), 9– 16. https://doi.org/10.1080/09540969 409387823

Gupta, S., & Bansal, A. (2020). Blockchain technology for transparent and secure transactions in e-government. *Government Information Quarterly, 37*(3), 101498. https://doi.org/10.1016/j.giq.2020.101498

Hood, C. (1991). A public management for all seasons? *Public Administration, 69*(1), 3–19. https://doi.org/10.1111/j.1467-9299.1991.tb00779.x

Laurent, M., & Moreau, A. (2018). Blockchain in public finance institutions: Enhancing resilience and auditability. *Public Management Review, 20*(6), 902– 920. https://doi.org/10.108 0/14719037.2017.1357967

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

OECD. (2018). *The path to becoming a data-driven public sector*. OECD Digital Government Studies. https://doi.org/10.1787/978926430763 6-en

Ofori, D., & Mensah, J. (2020). Blockchain and data security in Ghanaian government services. *Journal of African Public Administration, 6*(1), 15–32.

Park, J., Kim, H., & Lee, S. (2020). Blockchain and digital resilience in UK public agencies.

Information Systems Frontiers, 22(4), 939–953. https://doi.org/10.1007/s10796-020-10020-9

Rodriguez, M., & Scholl, H. J. (2018). Blockchain resilience in Brazilian public services. *International Journal of Public Administration in the Digital Age, 5*(3), 22–37. https://doi.org/10.4018/IJPADA.2018070102

Smith, A., & Johnson, K. (2019). Building trust and continuity through blockchain in local governments. *Public Administration Quarterly, 43*(1), 60–82.

Van Der Merwe, R. (2023). Digital infrastructure challenges to blockchain adoption in South Africa. *African Journal of Information Systems, 15*(1), 55–70.

Wang, H., & Li, Y. (2019). Decentralized resilience: Blockchain in Taiwan's public sector. *Government Studies Review, 31*(2), 201–218.

World Bank. (2017). *World development report 2017: Governance and the law*. World Bank. https://doi.org/10.1596/978-1-4648-0950-7

Yamane, T. (1967). *Statistics: An Introductory Analysis 2nd Ed*. Harper and Row, New York.

Zhang, Y., Chen, H., and Wang, L. (2019). Digital Literacy, Blockchain Adoption, and Service delivery: A Study in China. *Government Information Quarterly,* 36(3), p.p: 378-387.