PJ PALGO JOURNAL OF EDUCATION RESEARCH
ISSN 2476-8332
DOI : https://doi.org/10.65756/pjer.2026.006
Volume 11 Issue 2, June 2026.Page 33-38
http://www.palgojournals.org/PJER/Index.htm
Corresponding Author’s Email:mashungue@zou.ac.zw

Blockchain Technology for Ensuring Authenticity and Trust in Digital Records Management Systems in Zimbabwe.

Reason Gobvu[*1] and Edmore Mashungu[2]

Department of Information Science and Records Management Faculty of Applied Social Sciences, Zimbabwe Open University[1*]
Department of Educational Studies, Faculty of Education, Zimbabwe Open University[2]

Accepted ,June 23 , 2026

This empirical paper investigated blockchain technology for ensuring authenticity and trust in Digital Records Management Systems (DRMS) in Zimbabwe. The study objectives were to examine authenticity challenges in existing DRMS, assess blockchain's technical capabilities for evidential integrity, evaluate integration feasibility, and propose an implementation framework.A mixed-methods case study was adopted, using structured questionnaires with 134 records managers, IT officers, and auditors, and semi-structured interviews with 18 experts across 10 public institutions. Quantitative data were analysed with SPSS v28; qualitative data underwent thematic analysis in NVivo 14. The study was guided by the Records Trust Model and the DeLone & McLean IS Success Model. The population of the study was public sector records staff and IT professionals in Zimbabwe. Findings indicated that 78% of institutions faced disputed digital records due to weak audit trails. Blockchain’s immutable hashing and distributed consensus were rated highly for authenticity. A hybrid permissioned blockchain is feasible and legally compatible. The study concluded that blockchain enhances record trust but requires governance standards

Keywords: Blockchain, Digital records management, Authenticity, Trust, Immutability, Zimbabwe

1. **Introduction**

Digital transformation has redefined how governments create, manage, and use records, with Digital Records Management Systems (DRMS) now central to public administration, financial accountability, and service delivery (ISO, 2016). DRMS enable efficient capture, retrieval, and disposal of records while supporting compliance with legal and audit requirements (ARMA International, 2022). However, the shift from paper to digital has introduced persistent challenges of authenticity, integrity, and trust. Unlike physical records, digital records can be altered, deleted, or backdated without visible evidence, undermining their evidential value in courts, audits, and administrative processes (Lemieux, 2016; Bantin, 2018).

In Zimbabwe, public sector institutions managing high-value records such as payroll, pensions, land, and civil registration face acute authenticity risks. The Auditor-General of Zimbabwe (2022) has repeatedly flagged unverifiable digital transactions, disputed pension claims, and weak audit trails in government systems, eroding public trust and exposing the state to financial loss and litigation. Although the _Cyber and Data Protection Act [Chapter 12:07]_ mandates data integrity and security, conventional DRMS rely on centralized databases and administrator-controlled logs that remain vulnerable to insider manipulation, system breaches, and single points of failure (Zhang et al., 2021). As a result, stakeholders question whether digital records can be trusted as authentic evidence of transactions (Ngoepe, 2017).

Blockchain technology has emerged as a potential solution to this trust deficit. Defined as a distributed, cryptographically secured ledger, blockchain provides immutability, timestamping, and decentralized verification of data (Casino et al., 2019). By anchoring a record’s hash on a blockchain, organizations create tamper-evident proof of the record’s state at a specific time, enabling independent verification without relying on a single authority (Lemieux, 2020). International pilots in Estonia, Canada, and South Africa have demonstrated blockchain’s utility for land registries, academic credentials, and health records, reporting improved auditability and reduced fraud (Ølnes et al., 2017; Katuu, 2021).

Despite this promise, empirical research on blockchain in records management remains limited and largely technical. Most studies focus on proofs-of-concept with minimal evaluation of governance, legal admissibility, scalability, or integration with existing DRMS (Zhang et al., 2021). In Zimbabwe, no published research has assessed the feasibility, design requirements, or institutional readiness for blockchain-based authenticity controls in public sector DRMS. Critical questions persist: Can blockchain address authenticity without conflicting with data protection laws? How should it be integrated with legacy systems? What governance frameworks are needed for long-term preservation?

This study therefore investigates blockchain technology for ensuring authenticity and trust in Digital Records Management Systems in Zimbabwe. It examines current authenticity challenges, evaluates blockchain’s functional capabilities, assesses feasibility, and proposes a framework for implementation. Findings will inform policy, system design, and capacity building to strengthen evidential integrity and public trust in government digital records.

2.0 Literature Review

2.1 Authenticity and Trust Challenges in Digital Records Management Systems

Authenticity refers to a record being what it purports to be, free from tampering or corruption (ISO, 2016). Trust in digital records depends on demonstrable integrity, reliability, and provenance across time (Lemieux, 2016). Conventional DRMS use centralized access controls, audit logs, and checksums, yet these remain vulnerable. Administrator privilege abuse, weak segregation of duties, and mutable database logs enable undetectable alteration of records (Zhang et al., 2021). Bantin (2018) argues that centralized trust models fail because they require stakeholders to trust the system custodian rather than the record itself.

In the public sector, authenticity deficits have material consequences. Ngoepe (2017) documented cases in South Africa where disputed digital land and personnel records caused litigation due to absent audit trails. Mnjama (2018) found that 64% of ESARBICA institutions lacked tamper-evident controls, leading to parallel paper files as “legal backups.” In Zimbabwe, the Auditor-General (2022) cited unverifiable salary adjustments and missing pension records in DRMS, attributing this to inadequate logging and administrator-level access. Matangira and Ngulube (2019) confirmed that most Zimbabwean ministries cannot prove a digital record was unchanged since creation, reducing legal admissibility under the _Cyber and Data Protection Act [Chapter 12:07]_. Thus, authenticity in DRMS is both a technical and governance problem requiring independent verification mechanisms.

2.2 Technical Capabilities of Blockchain for Evidential Integrity

Blockchain is a distributed ledger where transactions are cryptographically hashed, timestamped, and linked in blocks verified by consensus (Casino et al., 2019). Three features are directly relevant to records authenticity.

i. **Immutability:** Once recorded, block data cannot be altered without altering all subsequent blocks, making tampering computationally infeasible (Ølnes et al., 2017).
ii. **Decentralized verification**: Multiple nodes hold copies, so trust shifts from a single administrator to network consensus (Lemieux, 2020).
iii. **Non-repudiation:** Private key signatures and timestamps provide proof of origin and time of commitment (Zhang et al., 2021).

Empirical tests confirm these capabilities. Lemieux (2016) demonstrated that hashing a record and storing the hash on Bitcoin’s blockchain created independently verifiable proof of existence and integrity. Katuu (2021) reported that South Africa’s blockchain land pilot reduced title fraud by enabling third-party verification of deed hashes. In health records, Zhang et al. (2021) found blockchain audit trails detected 100% of simulated tampering attempts, versus 62% for SQL-based logs. However, blockchain does not store records themselves due to size and privacy constraints; instead it anchors hashes or metadata “on-chain” while records remain “off-chain” in DRMS (Bantin, 2018). This hybrid model preserves performance and complies with data protection rules on erasure.

2.3. Feasibility of Integrating Blockchain with Existing DRMS

Feasibility depends on technical, legal, and organizational factors. Technically, APIs can link DRMS to permissioned blockchains such as Hyperledger Fabric or Corda, automating hash submission at record creation or finalization (Casino et al., 2019). Ølnes et al. (2017) documented Estonia’s integration of its X-Road DRMS with KSI Blockchain, achieving sub-second timestamping for 500 million transactions annually. Cost-benefit analyses show hybrid models avoid storing bulky records on-chain, reducing storage and transaction costs (Zhang et al., 2021).

Legally, blockchain timestamps are admissible under e-transaction laws in the EU and Canada, but Zimbabwean courts have not tested cryptographic proof (Lemieux, 2020). The _Cyber and Data Protection Act [Chapter 12:07]_ recognizes electronic signatures and data integrity, suggesting compatibility, though clarification on immutability versus right-to-erasure is needed (Government of Zimbabwe, 2021).

Organizationally, feasibility hinges on skills, infrastructure, and policy. Katuu (2021) noted that South African pilots failed when IT staff lacked blockchain competencies and when records policies did not define “authentic copy.” In Zimbabwe, Mutsagondo and Tsvuura (2021) found low digital preservation capacity, implying blockchain nodes would need external hosting or cloud services. Power and bandwidth instability may limit real-time anchoring, favoring batch hashing (Matangira & Ngulube, 2019).

2.4. Frameworks for Implementing Blockchain-Based Authenticity Controls

Several frameworks guide blockchain for records. Lemieux’s (2020) Records Trust Model posits that trust requires technological assurance, institutional legitimacy, and social acceptance. Blockchain addresses the first, but archival appraisal, retention, and legislation must address the latter two.

The InterPARES Trust Project (2018) proposed a Blockchain Records Management Framework with four layers: 1) Governance – policy, roles, legal basis; 2) Architecture – on-chain/off-chain design, node control; 3) Processes – when to hash, how to verify; 4) Preservation – long-term access to hashes and keys. Bantin (2018) added that appraisal must occur before blockchain commitment, since immutability conflicts with disposal.

In Africa, Katuu (2021) adapted this into a Blockchain Records Readiness Framework, emphasizing stakeholder buy-in, legislative mapping, and pilot testing. Key recommendations include using permissioned blockchains for confidentiality, appointing a “Trust Authority” to manage keys, and retaining hashes for as long as the record itself (ISO, 2020). No framework yet exists for Zimbabwe, indicating a gap this study seeks to fill.

Literature confirms that DRMS face authenticity deficits that blockchain can technically address through tamper-evident hashing and decentralized verification. Integration is feasible via hybrid models, but success depends on legal clarity, governance, and capacity. Existing frameworks provide a basis for a Zimbabwe-specific model that balances integrity, privacy, and preservation mandates.

3.0 Methodology

The study adopted a pragmatic mixed-methods case study design to assess blockchain technology for ensuring authenticity and trust in Digital Records Management Systems (DRMS) in Zimbabwe. The pragmatic paradigm was chosen because it allows integration of qualitative and quantitative approaches to address complex socio-technical problems where neither method alone is sufficient (Creswell & Plano Clark, 2018). A case study strategy was appropriate to investigate blockchain feasibility within the real-life context of Zimbabwe's public sector DRMS, where boundaries between the technology and institutional environment are not clear (Yin, 2018). The design was convergent parallel, meaning that quantitative and qualitative data were collected concurrently, analysed separately, and then integrated to corroborate findings."

The study was underpinned by two complementary theories: Records Trust Model (Lemieux, 2016) – explains how technological, institutional, and social mechanisms produce trust in records. Blockchain was positioned as a technological trust mechanism that provides cryptographic proof of integrity. DeLone and McLean Information Systems Success Model (DeLone & McLean, 2016) links system quality, information quality, and service quality to use, user satisfaction, and net benefits. Blockchain was conceptualized as enhancing system quality through immutability and auditability.

The target population comprised records managers, IT officers, system administrators, internal auditors, legal officers, and senior managers in Zimbabwean public institutions that operate DRMS for high-value records. Ten public institutions were purposively selected for managing critical records which included Salary Service Bureau, Deeds Registry, National Archives of Zimbabwe, Registrar General's Office, and 6 ministries.

A sample of 134 was obtained from a target population of 180 staff across the 10 sites, using stratified random sampling and Yamane's (1967) formula at 95% confidence level and ±5% margin, a sample of 134 was obtained. Purposive sampling was used to select 18 key informants, comprising 5 blockchain developers, 4 national archivists, 4 legal experts, and 5 senior DRMS administrators.

A structured questionnaire with 5-point Likert scales was used to measure perceptions of DRMS authenticity challenges, blockchain relevance, and feasibility. Items were adapted from Lemieux (2016) and Katuu (2021). These were administered online and in-person. Semi-structured interviews were also administered. Interviews lasted 30 to 45 minutes and were audio-recorded with consent (Saunders et al., 2019).

Document analysis was conducted on DRMS policies, audit reports, system logs, and legislation, including the Cyber and Data Protection Act [Chapter 12:07], to triangulate authenticity gaps (Bowen, 2009).

The instruments were pre-tested with 15 respondents from 2 institutions not in the main sample. Cronbach's alpha for the questionnaire was 0.86, indicating high internal reliability (Tavakol & Dennick, 2011). Interview questions were refined for clarity.

Quantitative data were coded and analysed using SPSS v28. Descriptive statistics summarize demographics and perceptions. Inferential tests, Chi-square and Spearman's rho, examined relationships between blockchain awareness and perceived feasibility (Field, 2018).

Qualitative interviews were transcribed verbatim and analysed thematically using NVivo 14, following Braun and Clarke's (2021) six-step process: familiarization, coding, theme generation, review, definition, and reporting.

Findings were merged at the interpretation stage to confirm, expand, or explain results. (Creswell & Plano Clark, 2018).

Content validity was ensured through expert review by 3 records management academics. Construct validity was tested via factor analysis. Reliability was confirmed with Cronbach's alpha > 0.70 (Saunders et al., 2019). Credibility was enhanced through member checking and triangulation. Dependability was ensured via an audit trail. Confirmability was addressed through reflexivity (Lincoln & Guba, 1985).

Informed consent, voluntary participation, anonymity, and confidentiality were observed (Bryman, 2016). Data were stored on encrypted drives. Participants were assigned codes to protect identities. The study complied with the Cyber and Data Protection Act [Chapter 12:07] regarding personal data.

The study was limited to public institutions in Harare due to cost. Findings may not generalize to local authorities or private sector. Blockchain technical testing was simulated, not live deployment, due to resource constraints.

4.0 Findings

This section presents results from the mixed-methods assessment of blockchain technology for ensuring authenticity and trust in Digital Records Management Systems (DRMS) in Zimbabwe. Data from 134 questionnaires, 18 interviews, and document analysis were integrated to address the four research objectives.

4.1 Demographic Profile of Respondents

Of the 134 questionnaire respondents, 54.5% were records officers, 28.4% IT/system administrators, 11.9% auditors, and 5.2% legal officers. 62.7% had more than 5 years' experience with DRMS."

4.1.1 Authenticity and Trust Challenges in Current DRMS
Quantitative

Prevalence of disputes: 78.4% (n=105) agreed/strongly agreed that their institution had experienced disputes over digital record authenticity in the past 3 years.
Audit trail weaknesses: 71.6% rated current DRMS audit logs as "inadequate" or "easily bypassed by administrators."
Top challenges
Administrator privilege abuse: M = 4.21, SD = 0.83
Lack of tamper-evident proof: M = 4.33, SD = 0.79
No independent verification: M = 4.18, SD = 0.91

Qualitative

Interviewees confirmed centralized control as the core vulnerability.
"Our DRMS has logs, but the system admin can edit the database directly. If they change a salary record and the log, who will know?" (R12, IT Manager)*"Courts ask us to prove a PDF payslip wasn't altered. We have no cryptographic proof, so we fall back to printing and stamping – which defeats the point of digital."* (R07, Legal Officer).
Document analysis
Auditor-General (2022) reports cited 3 ministries with unverifiable DRMS transactions worth ZWL$2.1 billion due to missing or overwritten audit trails.

4.1.2 Technical Capabilities of Blockchain for Evidential Integrity
Quantitative

Respondents rated blockchain features for authenticity on a 5-point scale:
Immutability: $M = 4.45$, $SD = 0.68$
Timestamping: $M = 4.38$, $SD = 0.72$
Decentralized verification: $M = 4.29$, $SD = 0.81$
Non-repudiation via digital signatures: $M = 4.31$, $SD = 0.76$
Spearman's rho showed significant positive correlation between blockchain awareness and perceived relevance for authenticity, $r = .612$, $p < .001$.

Qualitative

Developers and archivists validated the technical fit but stressed "off-chain" storage.
"You don't put the actual payslip on-chain. You hash it and store the hash. If anyone changes even a comma, the hash changes and verification fails. That's tamper-evident."([R03, Blockchain Developer)."*For legal admissibility, the hash + timestamp + node consensus gives us what wet-ink signatures gave paper – proof it existed and hasn't changed."*(R09, National Archivist)

4.1.3 Feasibility of Integrating Blockchain with Existing DRMS

Technical feasibility
Architecture preference: 83.6% supported a hybrid permissioned blockchain model where hashes are anchored on-chain while records stay in DRMS. Public blockchains were rejected by 76.1% due to data protection concerns.
Integration method: 67.9% indicated APIs could link current DRMS to Hyperledger Fabric with minimal disruption. Pilot simulations showed hash anchoring added <1.2s to record finalization.
Legal feasibility
Legal experts agreed blockchain evidence is consistent with Cyber and Data Protection Act [Chapter 12:07] s.13 on electronic records integrity. However, 88.9% noted gaps: no provisions for "immutable record" or conflict with right-to-erasure.
"The Act allows functional equivalence. If we can show a hash proves integrity, courts should accept it. But we need regulations defining cryptographic proof." (R15, Legal Expert)
Organizational feasibility
Barriers: Cost ($M = 4.11$), skills gap ($M = 4.03$), power/bandwidth instability ($M = 3.89$).
Enablers: 72.4% said government cloud infrastructure could host nodes. 64.2% reported senior management would support pilots if donor-funded.
Chi-square test
Institutions with ISO 27001 certification were significantly more likely to rate integration as feasible, $\chi^2(1, N=134) = 9.47$, $p = .002$.

4.1.4 Framework for Implementation

Interview and survey data converged on a 4-layer implementation framework:
Governance Layer
Amend National Archives Act to recognize cryptographic hashes as "authentic copies."
Establish National Archives as "Trust Authority" to manage blockchain nodes and keys.
Retention schedules must precede hashing; immutable data cannot be legally disposed.
Architecture Layer
Permissioned blockchain (Hyperledger Fabric) with nodes at National Archives, Ministry of Finance, and Auditor-General.
Off-chain DRMS stores records; on-chain stores SHA-256 hash, timestamp, and record ID only.
Process Layer:
Hash records at point of "finalization" for example, after payroll approval.
Verification portal for public/third parties to check hash without accessing record content.
Key management policy for long-term preservation >50 years.
Capacity Layer
Training for 200+ records/IT staff on blockchain RM.
Pilot at Salary Service Bureau for payslips and Deeds Registry for title deeds.
88.9% of key informants endorsed the framework as "practical" provided legal reforms precede rollout.

4.2 Integration of Findings

Triangulation confirmed that DRMS authenticity deficits are real, measurable, and costly. Blockchain's immutability directly addresses the identified gap of tamper-evident proof. Hybrid architecture resolves privacy and scalability concerns. However, legal and skills barriers must be addressed before benefits are realized. Institutions with stronger IT governance showed higher readiness.

5.0 Discussion

5.1 Authenticity and Trust Deficits in Current DRMS

The finding that 78% of institutions experienced disputes over digital record authenticity confirms that trust in DRMS remains a systemic problem in Zimbabwe's public sector. This aligns with Lemieux's (2016) assertion that centralized DRMS shift trust from the record to the custodian, creating a single point of failure. The high mean scores for "administrator privilege abuse" (M = 4.21) and "lack of tamper-evident proof" (M = 4.33) mirror challenges reported in South Africa and Kenya where database-level edits undermined audit trails (Ngoepe, 2017; Mnjama, 2018). The Auditor-General's (2022) citation of ZWL$2.1 billion in unverifiable transactions provides empirical weight to Bantin's (2018) warning that DRMS without independent verification mechanisms risk financial and legal exposure. Thus, the study validates that current DRMS cannot demonstrably guarantee evidential integrity, eroding institutional and public trust.

5.2 Blockchain's Technical Capabilities for Evidential Integrity

Respondents rated blockchain's immutability (M = 4.45) and timestamping (M = 4.38) as highly relevant, supporting Casino et al.'s (2019) claim that cryptographic hashing provides "computational trust." The qualitative theme of "hash proves existence without revealing content" resolves the privacy dilemma noted by Zhang et al. (2021) — records stay off-chain while hashes provide tamper-evidence. This corroborates Lemieux's (2020) Records Trust Model: blockchain strengthens the _technological_ trust layer without requiring trust in any single administrator. The significant correlation between blockchain awareness and perceived relevance ($r = .612$, $p < .001$) suggests that capacity building is a prerequisite for adoption, echoing Katuu's (2021) findings in South Africa where low awareness delayed pilots. Therefore, blockchain technically addresses authenticity, but only through hybrid on-chain/off-chain design.

5.3 Feasibility of DRMS-Blockchain Integration

The preference for permissioned Hyperledger Fabric (83.6%) over public chains addresses legal and confidentiality concerns raised by Ølnes et al. (2017) and aligns with Estonia's KSI Blockchain model. The <1.2s latency for hash anchoring indicates technical feasibility without disrupting DRMS performance, supporting Zhang et al.'s (2021) scalability claims. Legal experts' view that the Cyber and Data Protection Act [Chapter 12:07] supports functional equivalence is important, yet the identified gap on "immutable record versus right-to-erasure" confirms Bantin's (2018) warning The finding that ISO 27001-certified institutions rated integration more feasible ($p = .002$) links to DeLone and McLean's (2016) IS Success Model, system quality and organizational maturity drive net benefits. Cost, skills, and infrastructure barriers mirror Mnjama (2018) and Matangira & Ngulube (2019), suggesting Zimbabwe shares regional constraints. Thus, integration is feasible but conditional on legal reform and capacity investment.

5.4 Framework for Implementation

The emergent four-layer framework — comprising Governance, Architecture, Process, and Capacity — extends InterPARES Trust's (2018*) model* by contextualizing it for Zimbabwe's legal and infrastructural realities. The designation of National Archives as "Trust Authority" addresses Lemieux's (2020) requirement for institutional legitimacy beyond technology. The rule that "retention precedes hashing" directly responds to Bantin's (2018) preservation paradox: immutability conflicts with disposal unless appraisal occurs first. The pilot recommendation for SSB payslips and Deeds Registry aligns with Katuu's (2021) advice to start with high-value, high-risk records. Endorsement by 88.9% of experts indicates stakeholder buy-in, satisfying the social trust dimension of the Records Trust Model. Objective 4 is therefore achieved with an evidence-based, locally adapted framework.

6.0 Conclusion

This study concluded that Digital Records Management Systems in Zimbabwe face acute authenticity and trust deficits due to centralized architectures vulnerable to undetected alteration. Blockchain technology, through immutable hashing, timestamping, and decentralized verification, provides a technically viable mechanism to create tamper-evident proof of record integrity without compromising privacy or performance.

A hybrid permissioned blockchain model is feasible and legally compatible with the Cyber and Data Protection Act [Chapter 12:07], provided regulations are amended to recognize cryptographic proof and clarify conflicts with data erasure rights. Feasibility is highest in institutions with mature IT governance, but national rollout is constrained by costs, skills gaps, and infrastructure instability. The proposed 4-layer implementation framework offers a practical pathway: establishing governance and legal clarity, adopting permissioned architecture, anchoring hashes at finalization, and building capacity through targeted pilots. Blockchain is not a panacea and cannot replace records management fundamentals of appraisal, classification, and retention. However, as a trust infrastructure layer, it materially strengthens evidential integrity, legal admissibility, and public confidence in government digital records. Future research should conduct live pilots at Salary Service Bureau and evaluate long-term preservation of blockchain-anchored records beyond 30 years.

References

ARMA International. (2022). Information governance benchmark report. ARMA International. https://www.pathlms.com/arma-international/courses/71624

Auditor-General of Zimbabwe. (2022). _Report of the Auditor-General for the financial year ended December 31, 2021_. Government of Zimbabwe. Available at: https://veritaszim.net/node/6048

Bantin, P. C. (2018). Blockchain and records management: Disruptive force or new tool? _Archives and Manuscripts, 46_(2), 142–158. https://doi.org/10.1080/01576895.2018.1502082

Bowen, G. A. (2009). Document analysis as a qualitative research method. _Qualitative Research Journal, 9_(2), 27–40. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2021). _Thematic analysis: A practical guide_. SAGE. https://uk.sagepub.com/en-gb/eur/thematic-analysis/book248481

Bryman, A. (2016). _Social research methods_ (5th ed.). Oxford University Press. https://www.biblio.com/9780199689453

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. _Telematics and Informatics, 36_, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Creswell, J. W., & Plano Clark, V. L. (2018). _Designing and conducting mixed methods research_ (3rd ed.). SAGE. https://study.sagepub.com/creswell3e

Creswell, J. W., & Poth, C. N. (2018). _Qualitative inquiry and research design: Choosing among five approaches_ (4th ed.). SAGE. https://uk.sagepub.com/en-gb/eur/qualitative-inquiry-and-research-design/book266033

DeLone, W. H., & McLean, E. R. (2016). Information systems success measurement. _Foundations and Trends in Information Systems, 2_(1), 1–116. https://doi.org/10.1561/2900000005

Field, A. (2018). _Discovering statistics using IBM SPSS statistics_ (5th ed.). SAGE. https://uk.sagepub.com/en-gb/eur/discovering-statistics-using-ibm-spss-statistics/book285130

Government of Zimbabwe. (2021). _Cyber and Data Protection Act [Chapter 12:07]_. Government Printer. https://www.veritaszim.net/node/5522

International Organization for Standardization. (2016). _ISO 15489-1:2016 Information and documentation — Records management — Part 1: Concepts and principles_. ISO. https://www.iso.org/standard/62542.html

International Organization for Standardization. (2020). _ISO 16175-2:2020 Information and documentation — Processes and functional requirements for software for managing records — Part 2: Guidance_. ISO. https://www.naa.gov.au/information-management/standards/iso-16175-what-you-need-know

InterPARES Trust. (2018). _Blockchain research findings_. University of British Columbia.

Katuu, S. (2021). Blockchain and records management: The South African perspective. _Records Management Journal, 31_(2), 173–190. https://doi.org/10.1108/RMJ-08-2020-0030

Lemieux, V. L. (2016). Trusting records: Is blockchain technology the answer? _Records Management Journal, 26_(2), 110–139. https://doi.org/10.1108/RMJ-12-2015-0042

Lemieux, V. L. (2020). _Searching for trust: Blockchain technology in an age of disinformation_. Cambridge University Press.

Lincoln, Y. S., & Guba, E. G. (1985). _Naturalistic inquiry_. SAGE.

Matangira, V., & Ngulube, P. (2019). Records management and service delivery in Zimbabwe's public sector. _ESARBICA Journal, 38_, 1–19.

Mnjama, N. (2018). E-records readiness in Africa. _Records Management Journal, 28_(2), 146–160. https://doi.org/10.1108/RMJ-02-2018-0006

Mutsagondo, S., & Tsvuura, G. (2021). Utilisation of electronic records management systems at the Zimbabwe Revenue Authority. _Journal of the South African Society of Archivists, 54_, 45–60.

Ngoepe, M. (2017). Archives and public sector accountability in Africa. _Journal of the South African Society of Archivists, 50_, 1–15.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. _Government Information Quarterly, 34_(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007

Saunders, M., Lewis, P., & Thornhill, A. (2019). _Research methods for business students_ (8th ed.). Pearson.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. _International Journal of Medical Education, 2_, 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd

Yamane, T. (1967). _Statistics: An introductory analysis_ (2nd ed.). Harper & Row.

Yin, R. K. (2018). _Case study research and applications: Design and methods_ (6th ed.). SAGE.

Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2021). Blockchain technology use cases in records management: A systematic review. _IEEE Access, 9_, 88122–88141. https://doi.org/10.1109/ACCESS.2021.3089170