International Research Journal of Rongo University (IJORU) ISSN: 3005-7221
Transformative Research and Innovation for an Inclusive and Sustainable Future
Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

EMPIRICALLY DERIVED DESIGN REQUIREMENTS FOR A BLOCKCHAIN-BASED ENTERPRISE RESOURCE PLANNING SECURITY FRAMEWORK: EVIDENCE FROM SELECTED WATER AND SANITATION COMPANIES IN KENYA

[1]Dennis Boera Onchwari*, [1]Lamek Ronoh, [1]James Abila

*Corresponding Author: dennisboera@gmail.com

https://orcid.org/0009-0005-6987-9863; https://orcid.org/0000-0003-0385-280X; https://orcid.org/0000-0003-0805-214X

[1]Rongo University, P.O. Box 103-40404 Rongo, Kenya

Abstract

Requirements engineering plays an important role in Design Science Research (DSR) as it is a process that makes organizational problems into implementable design artefacts. Previous research on blockchain-based Enterprise Resource Planning (ERP) security is mostly concerned with technology architecture, adoption and implementation obstacles, and less with systematic mapping of empirical evidence into traceable engineering specifications and design requirements. The current study suggests a requirements engineering based approach to the development of the ERP security framework in the DSR context using evidence. In two public water and sanitation companies (PWSC) in Kenya, a pragmatic philosophy was employed and a mixed-methods approach and descriptive research design used. The data were collected using a census of 43 ERP users, and 39 valid questionnaire responses (90.7%) were attained, plus semi-structured interviews, document reviews and system observations. Descriptive statistics, Pearson's Chi-square and Fisher's Exact Test were used for analyzing quantitative data and thematic analysis for qualitative data which were further integrated through triangulation procedure. The results showed significant issues with transaction integrity, auditability, identity and access control, interoperability, and governance. Blockchain platform readiness was significantly related to cross module consistency ($\chi^2 = 12.042$, $p = .001$) and other tested relationships were less significant. A structured requirement engineering process was used to systematically transform empirical findings to the requirements of stakeholders, engineering specifications and design requirements. The study is a step towards DSR as it provides evidence-based path to move organizational problems to design requirements of blockchain-based ERP security.

Keywords: *Enterprise Resource Planning; Blockchain technology; Design Science Research; ERP security; Distributed Ledger Technology; Design requirements.*

Introduction

ERP (Enterprise Resource Planning) systems are applications that connect important business activities to a single information platform, which can be used for optimizing resources, streamlining business processes, sharing information and making decisions. ERP systems connect various business functions, such as finance, procurement, inventory, HR, customer relationship management, billing, supply chain management, and asset management, all in one place and in a standardized way (Jacobs & Weston, 2007; Kumar et al., 2023). This makes ERP a key component of the digital transformation process in both private and public sector companies. But due to their centralized nature and the storing and use of mission-critical data and business transactions, ERP systems are susceptible to cybersecurity risks. Insider threats, ransomware, poor segregation of duties, inconsistent metadata, weak authentication, inadequate audit trails and excessive privileges can impact the confidentiality, integrity and availability of information (International Organization for Standardization [ISO], 2022b; National Institute of

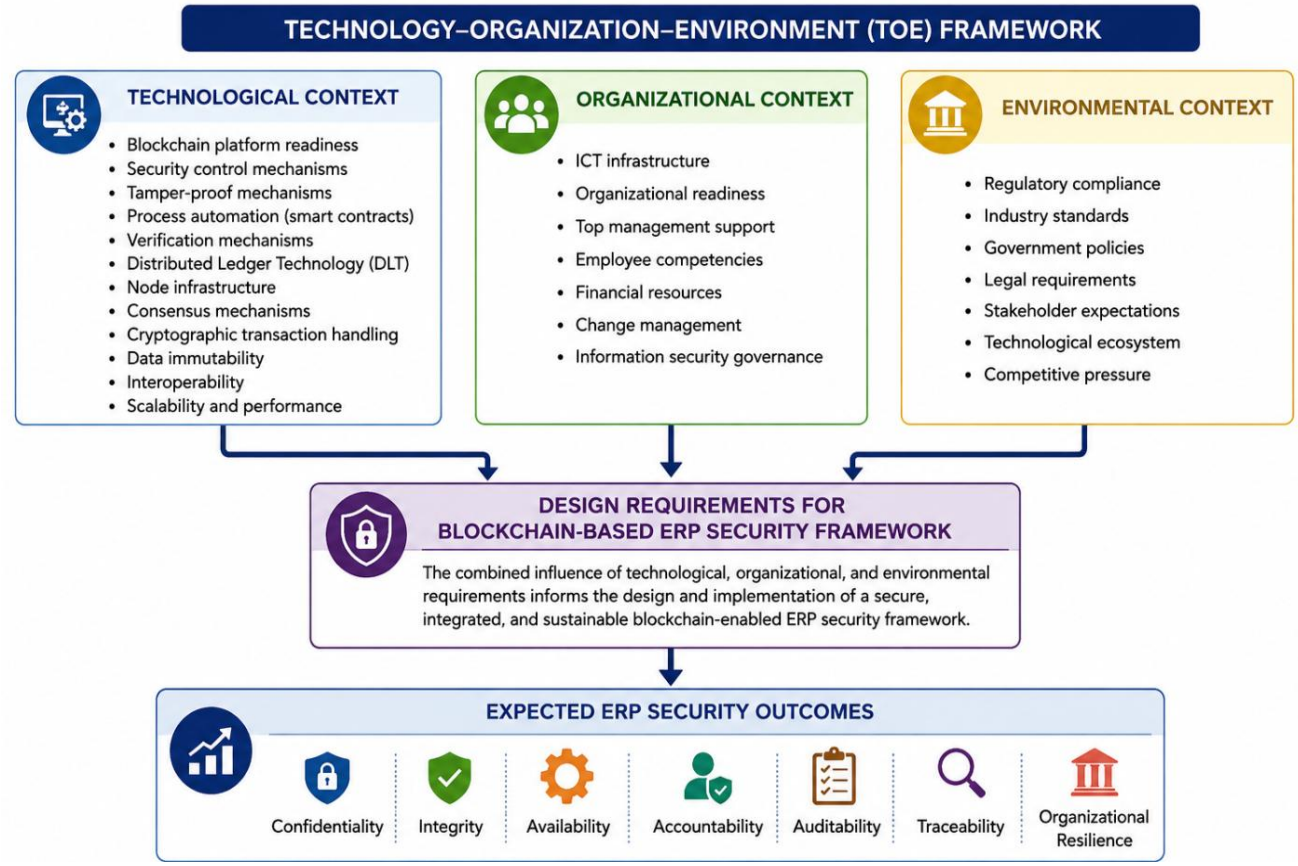
Standards and Technology [NIST], 2024). In public sector organizations, ERP systems play a crucial role in supporting various functions, such as financial management, procurement, revenue collection, regulatory compliance, and critical service operations, making these risks especially significant. The attack surface is even larger with the integration of cloud computing, mobile platforms, the Internet of Things (IoT) and third-party applications, resulting in interoperability and governance issues as well (Casino et al., 2019). Threat intelligence has also revealed that business-critical ERP applications can be the victims of ransomware and suffer significant operational disruption as a result of traditional endpoint security and backup solutions (Onapsis, 2021). These risks underscore the need for system access controls as well as transaction integrity, auditability, traceability and accountability controls. Blockchain technology has proven its usefulness as an ERP complement to provide additional security in certain aspects. Blockchain is a decentralized ledger technology (DLT) that offers decentralized verification, cryptographic protection, tamper-resistant transaction record, smart-contract automation, and transaction traceability (Casino et al., 2019; Isbaih et al., 2024). These capabilities can be used to add to the existing ERP infrastructure as a verification and integrity layer. As a result, the blockchain applications are gaining traction in various enterprise information systems such as healthcare, supply chains, public administration, and finance (Yue et al., 2022; Zheng et al., 2017). Blockchain, however, is not the solution to ERP security, though. It is interoperable with legacy ERP systems, has governance controls, identity and key management, consensus procedures, scalability, performance, regulatory compliance and organizational readiness features (Casino et al., 2019; Kumar et al., 2023; Sunmola & Lawrence, 2024). It also doesn't fix information inaccuracies that occur at the time it enters the system, which makes authentication, authorization, transaction validation, data quality and governance critical. All of these factors suggest that before implementing blockchain, there needs to be careful analysis and validation of what it is expected to achieve for the organization and what its organizational and technical needs are. Previous studies have explored the blockchain use in enterprise systems such as supply chain, accounting, security, traceability, purchasing, process automation, blockchain–ERP integration (Isbaih et al., 2024; Sunmola & Lawrence, 2024). Far less study have focused however on the systematic process of transforming the ERP security issues observed in the field into the needs of stakeholders, engineering specifications, and actionable design needs. Most studies typically provide a description of blockchain requirements as abstract capabilities or as an extension of requirements from other frameworks without describing how they have been found in the field within operational organizational environments. Despite the vast knowledge about the capabilities of blockchain and the integration challenges, there is limited guidance in the literature on how to transform empirical security problems in ERP to evidence-based design requirements. Requirements Engineering (RE) is a systematic process for gathering, analyzing, specifying, checking and handling the requirements of stakeholders and organizations (Sommerville, 2016; Wiegers & Beatty, 2013). In Design Science Research (DSR), RE can offer a methodological bridge between problem investigation in an empirical way and the creation of artefacts. DSR focuses on the development of artefacts to address problems identified within an organization and to produce design knowledge that can be beneficial to the organization (Hevner et al., 2004; Peffers et al., 2007). But, in contrast, very few DSR studies clearly articulate the relationship between the empirical findings and the engineering specifications prior to construction of the artefacts. This transformation can be helpful in enhancing methodological transparency, the possibility of reproducing and tracing. Based on the above, this research suggests an evidence-based requirements engineering method for developing the security framework for ERP using the blockchain in DSR. The method combines quantitative results, qualitative evidence, organizational documents, system observations, security standards, and domain literature to map the identified organizational problems to the requirements of the stakeholders, then to engineering specifications and design requirements. This is especially true in enterprise cybersecurity, where security issues occur as a result of the interplay between the technical vulnerabilities, the organization,

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

governance, regulation and human behavior. The study is based on the Technology – Organization – Environment (TOE) framework created by Tornatzky and Fleischer (1990) which outlines how people adopt technology, based on technological, organizational and environmental factors (Baker, 2012). The technological dimension includes ERP infrastructure, interoperability, data integrity, security controls and the ability of ERP systems to include blockchain; the organizational dimension includes readiness, governance, human resources and organizational practices; whereas the environmental dimension includes regulatory, institutional and external factors. The framework is used to inform the selection of variables, data collection, analysis, interpretation and generation of evidence-based design requirements.

Figure 1

Conceptual framework illustrating the technological, organizational, and environmental dimensions underpinning the derivation of design requirements for a blockchain-based Enterprise Resource Planning (ERP) security framework



In order to derive empirically grounded design requirements for a blockchain-based ERP security framework, the TOE framework is operationalized in Figure 1 by exploring the relationship between technological and organizational factors that shape blockchain integration requirements and the environmental factors that shape the integration of blockchain in ERP. The frame work was used to select the variables, collect the data, analyze the data and interpret the meaning of the data. It is found from the reviewed literature that there is a gap between the empirical organizational evidence and knowledge of implementable design. While there is substantial research that guides the security of ERP, blockchain capabilities, blockchain–ERP integration and DSR, little research has focused on a transparent process for translating observed security issues into requirements of the stakeholders, engineering requirements, and

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

implementable design requirements. The relevance and utility of a DSR artefact requires the ability to show how the design decisions have been made to relate to the organizational issues that it solves. In a nutshell, the research examines the integration requirements for ERP in blockchain in the context of Kenya's case study of the Gusii Water and Sanitation Company (GWASCO) and Kericho Water and Sanitation Company (KEWASCO). Specifically, it evaluates technological, organizational and governance requirements for the integration of blockchain; explores the interaction between ERP data-integrity attributes and blockchain system requirements; and studies the requirements for a blockchain-based ERP security framework, based on empirical findings. An EBP process takes the empirical results and converts them to the requirements of the stakeholders, engineering requirements and implementable design requirements. It is not only the use of blockchain as a security mechanism for ERP, but also the systematic application of the empirical evidence of the organizations to traceable engineering specifications to be followed when building artefacts in DSR. The study adds engineering specificities as an intermediate abstraction layer to enhance the methodological transparency, traceability and reproducibility while offering some practical recommendations for secure integration of the blockchain in public sector enterprise information systems.

Research Methodology

The research philosophy used in this study was pragmatic research, which is used when selecting research methods based on the suitability of the methods needed to solve practical research problems (Creswell & Creswell, 2023; Saunders et al., 2023). It was suitable, as the study utilised both quantitative and qualitative evidence to explore ERP security issues and identify requirements for the integration of blockchain into ERP (Tashakkori & Teddlie, 2021). The quantitative evidence identified security issues and security needs, and the qualitative evidence contributed to determining why and how the stakeholder experienced security issues, and how their security issues were being addressed, as well as the organization's practices, governance and operational challenges. The integrated evidence informed the process of moving from empirical evidence to stakeholder needs, engineering requirements, and design requirements that could be implemented in DSR. The mixed methods with descriptive research design were used in the DSR paradigm. The descriptive design was used to describe the current ERP security picture, without manipulating study variables, such as security of data integrity, access control, auditability, interoperability, blockchain readiness, and governance (Creswell & Creswell, 2023; Saunders et al., 2023). A causal design was not used because it was not the main purpose; also, an exploratory design alone would not give the quantitative evidence necessary to establish the prevalence of identified deficiencies. Design Science Research Methodology (DSRM) of Peffers et al. (2007) was used to guide the DSR component. Empirical problem investigation led to design objects and the needs of stakeholders were translated into engineering specifications and functional and non-functional design requirements. Requirements Engineering was thus used to create a methodological connection between empirical investigation and artefact development. The study was carried out at two purposively selected water and sanitation companies, namely Gusii Water and Sanitation Company (GWASCO) and Kericho Water and Sanitation Company (KEWASCO), which has an ERP environment that supports interconnected processes in the Water and Sanitation sector such as Finance, Procurement, Billing, Revenue Management, Inventory, Customer Relationship Management, Asset Management and Human Resources. Thus, the context was suitable for exploring the needs for ERP security, accountability, auditing and blockchain integration. The results are most relevant to public sector and other regulated organizations that have similar ERP environments. Target population included all 43 ERP users and stakeholders, encompassing ERP administration, management, auditing and operational use within the two organizations. This entailed using a census approach as it was the total defined target population (Kothari, 2004; Mugenda & Mugenda, 2003). There was a response rate of 90.7% (39 questionnaires completed). For quantitative analysis, there were 39 valid responses, and 14 ICT managers, ERP administrators, internal auditors and senior managers who were involved in a semi-structured interview. The

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

data collection methods were semi-structured interviews, structured questionnaires, observation checklists, document reviews of the organizations, system log analysis and vulnerability assessment. The questionnaire encompassed ERP security and blockchain integration needs, such as platform readiness, security measures, tamper resistance, process automation, DLT readiness, node infrastructure, consensus mechanisms, cryptographic transaction management, interoperability, scalability, governance and regulatory compliance. Interviews offered contextual evidence for security practices, governance, organizational readiness, challenges to implementation, and stakeholder expectations. Observations, documents, system logs, and vulnerability assessments were used to complement the findings of methodological triangulation and comparing reported conditions with documented and observed characteristics of systems. A Requirements Engineering process that was based on evidence resulted in design knowledge. Using quantitative and qualitative data, recurring and corroborated security issues were identified and stated as stakeholder needs, and finally converted into technology-neutral engineering specifications detailing the capabilities needed to solve the issues. The specifications were then converted into functional and non-functional design requirements of the proposed framework for blockchain-based ERP security, which then linked empirical evidence to design requirements. Content validity was achieved by subjecting the instrument to expert validation by the two study supervisors who are both PhD holders and Senior Lecturers in Information Technology, Rongo University. They evaluated the relevance, clarity, completeness and congruence of the items in the questionnaire and the interview with the research goals and constructs. Their comments helped to make changes prior to the main study. Ambiguities were also identified through a pilot study, helping to clarify the instruments and data collection procedures. Cronbach's alpha was calculated for internal consistency reliability of the instruments, all the alpha values were above 0.70 (Cronbach, 1951; Taber, 2018). IBM SPSS Statistics Version 27 was used for analysing quantitative data. ERP security conditions and blockchain integration requirements were summarized in frequencies, percentages, means and SDs. Pearson's Chi-square test was used to analyze association between categorical data-integrity attributes from ERP and blockchain integration requirement, and Fisher's Exact test used in cases where the expected frequency of cells was not large enough for Pearson's Chi-square test. Association strength was measured using Cramer's V and their significance was determined at the level of $\alpha = 0.05$ (Agresti, 2019).

Results and Discussion

We now discuss the empirical results of the requirements for integrating blockchain into Enterprise Resource Planning (ERP) systems. Results are descriptive and inferential analyses. Descriptive analysis provides an overview of the state of blockchain integration preparedness and inferential analysis investigates the relationships between the attributes of ERP data and the requirements for blockchain integration. The findings are combined to obtain empirical basis for the design requirements for the proposed blockchain-based ERP security framework.Considering all the findings; the design requirements for the proposed blockchain-based ERP security framework are derived.

Descriptive Analysis of Blockchain Integration Requirements

Through descriptive analysis, the study assessed blockchain integration readiness within the ERP environments of the participating organizations. The findings were grouped into four technological domains. Blockchain platform readiness, Distributed Ledger Technology (DLT) readiness, node infrastructure, and node discovery capability were assessed to determine platform and infrastructure readiness. Table 1 presents the results.

Blockchain Platform and Infrastructure Readiness

Blockchain platform and infrastructure readiness was assessed using indicators of blockchain platform readiness, Distributed Ledger Technology (DLT) readiness, node infrastructure, and node discovery capability. Table 1 presents the results.

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

Table 1

Blockchain platform and infrastructure readiness for Enterprise Resource Planning integration

Technological requirement	Current readiness (%)	International benchmark (%)	Gap (%)	Assessment
Blockchain platform readiness	28.0	≥90	62.0	Low readiness
Distributed Ledger Technology readiness	28.0	≥90	62.0	Low readiness
Node infrastructure	77.8	≥90	12.2	Moderate readiness
Node discovery capability	72.2	≥90	17.8	Moderate readiness

The findings show significant differences in blockchain applications' technological readiness when integrating with ERP. Blockchain platform readiness and DLT readiness both scored 28.0%, which is 62.0 percentage points short of the ≥90% target. With gaps of 12.2 percentage points and 17.8 percentage points, respectively, node infrastructure and node discovery showed the highest readiness levels of 77.8% and 72.2%, respectively. But both were still below the standards. This shows that the ICT infrastructure currently in place was relatively well developed compared to blockchain-related skills. Therefore, having the proper infrastructure base does not always mean that they were prepared for the use of DLT. The blockchain platform and DLT technologies were thus the most salient technological gaps and requirements for the next engineering specifications.

Security Control and Transaction Integrity Requirements

Security control and transaction integrity were evaluated based on indicators of security controls, tamper proof mechanisms, transaction verification. The results are given in Table 2.

Table 2

Security control and transaction integrity requirements for blockchain-enabled Enterprise Resource Planning systems

Technological requirement	Current readiness (%)	International benchmark (%)	Gap (%)	Assessment
Security control mechanisms	20.5	≥90	69.5	Critical deficiency
Tamper-proof mechanisms	10.3	≥95	84.7	Critical deficiency
Transaction verification	33.0	≥95	62.0	Low readiness

The results show that there are significant gaps in the security features that are needed to safeguard ERP transactions and ensure data integrity. Security control mechanisms had a Moderate level of readiness, with 20.5% of respondents reporting a readiness of ≥90%. The lowest level of readiness was for tamper-proof mechanisms, which recorded 10.3%, and had an 84.7-percentage point gap from the ≥95% threshold. 33.0% of transactions were ready, which is still 62.0 percentage points short of ≥95%. The findings show that there is not much preparedness for mechanisms that offer tamper resistance and independent transaction verification. The exceptionally low tamper-proof and transaction-verification scores reflect a lack of integrity and accountability in transactions. These findings agree with the need for a mandatory permanent record of transactions, cryptographic security, distributed verification of transactions, and audit capabilities that will provide evidence of tampering within the proposed framework.

Business Process Automation Requirements

The business process automation was evaluated to understand the degree of automation of the transactions and business rules in place in the current ERP environments for integration with blockchain. The results have been summarized in Table 3.

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

Table 3

Business process automation requirements for blockchain-enabled Enterprise Resource Planning systems

Technological requirement	Current readiness (%)	International benchmark (%)	Gap (%)	Assessment
ERP business process automation	25.0	≥80	55.0	Low readiness

The results indicate that ERP business process automation had a score of 25.0%, which is 55.0 percentage points lower than the ≥80% threshold. This means that there is low readiness for automated ERP processes and manual intervention is still necessary to execute ERP processes. The low readiness further indicates that there is no extensive automation possible due to the lack of standardization and digitization of the existing processes. The discovery underscores the need for business process automation in ERP integration with blockchain, especially by leveraging standardized digital workflows and automated execution processes that enable consistent, compliant, and auditable transactions.

Consensus Governance and Cryptographic Security Requirements

Consensus validity, validator selection, consensus readiness, cryptographic controls, key management, tamper evident logging and cryptographic readiness were determined and analyzed through consensus indicators. The outcomes are given in Table 4.

Table 4

Consensus governance and cryptographic security requirements for blockchain-enabled Enterprise Resource Planning systems

Technological requirement	Current readiness (%)	International benchmark (%)	Gap (%)	Assessment
Consensus validity	36.0	≥90	54.0	Deficient
Validator selection	40.0	≥90	50.0	Deficient
Overall consensus readiness	38.0	≥90	52.0	Deficient
Cryptographic controls	13.0	≥95	82.0	Not ready
Cryptographic key management	9.0	≥90	81.0	Not ready
Tamper-evident logging	13.0	≥95	82.0	Not ready
Overall cryptographic readiness	12.0	≥90	78.0	Significantly not ready

The findings suggest that the governance and cryptographic skills necessary for blockchain-based ERP are not well prepared. The consensus readiness was 38.0% with consensus validity of 36.0% and selection of validators of 40.0% indicating gaps of 52.0%, 54.0%, and 50.0% respectively from the ≥90% threshold. Cryptographic readiness was much lower, with overall readiness at 12.0% compared to ≥90% target of 78.0 percentage points. Cryptographic controls and tamper evident logging both had a 13.0% level of readiness, falling 82.0 and 82.0 percentage points short, respectively, of the 100% mark. Key management had 9.0% readiness, 81.0 percentage points short of the 100% mark. The findings reveal that the following are key requirements of secure transaction validation, integrity and accountability: Cryptographic protection, Key management, Consensus governance, Validator management, Tamper evident logging..

Inferential Analysis

The relationships between data-integrity attributes of ERP and blockchain integration requirements were analyzed using inferential analysis. Categorical variables were analyzed by Pearson's Chi-square test, and Fisher's Exact Test was used when the expected cell frequencies were low. Significant relationships were determined at $\alpha = 0.05$ and Cramer's V was used to measure the strength of significant relationships.

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

Table 5

Inferential analysis of relationships between ERP data integrity attributes and blockchain integration requirements

ERP integrity attribute	Blockchain requirement	Statistical test	Test statistic	*p*-value	Interpretation
Accuracy and completeness	Platform readiness	Fisher's Exact Test	—	.721	Not significant
Metadata completeness	Cryptographic safeguards	Pearson's χ^2	0.412	.521	Not significant
Audit-trail completeness	Transaction handling	Pearson's χ^2	0.396	.529	Not significant
Cross-module consistency	Platform readiness	Pearson's χ^2	12.042	.001	Significant
Access-control integrity	Authentication controls	Pearson's χ^2	0.583	.445	Not significant
Distributed ledger requirements	Consensus mechanisms	Pearson's χ^2	0.068	.795	Not significant

The results of the analysis have revealed that there is a moderate association between cross-module consistency and platform readiness ($\chi^2 = 12.042$, $p = .001$, Cramer's $V = .333$) while the other two associations do not meet the criteria for being significant. No other relationships were statistically significant ($p > .05$). The high association indicates that readiness of the platform is a crucial factor when dealing with consistency between interrelated ERP modules. All of these inferential results along with the descriptive results were used to come up with the stakeholder requirements and engineering specifications.

Empirically Derived Design Requirements for a Blockchain-Based Enterprise Resource Planning Security Framework.

The synthesis of descriptive and inferential findings was used to arrive at design requirements for a proposed security framework using blockchain in the ERP system. The requirements are technological, security, governance and operational capabilities that should be met to address identified ERP security shortcomings. The derivation was done using the Requirements Engineering process, based on an evidence based approach that connects the empirical findings to requirements for design, which are implementable and technological gaps.

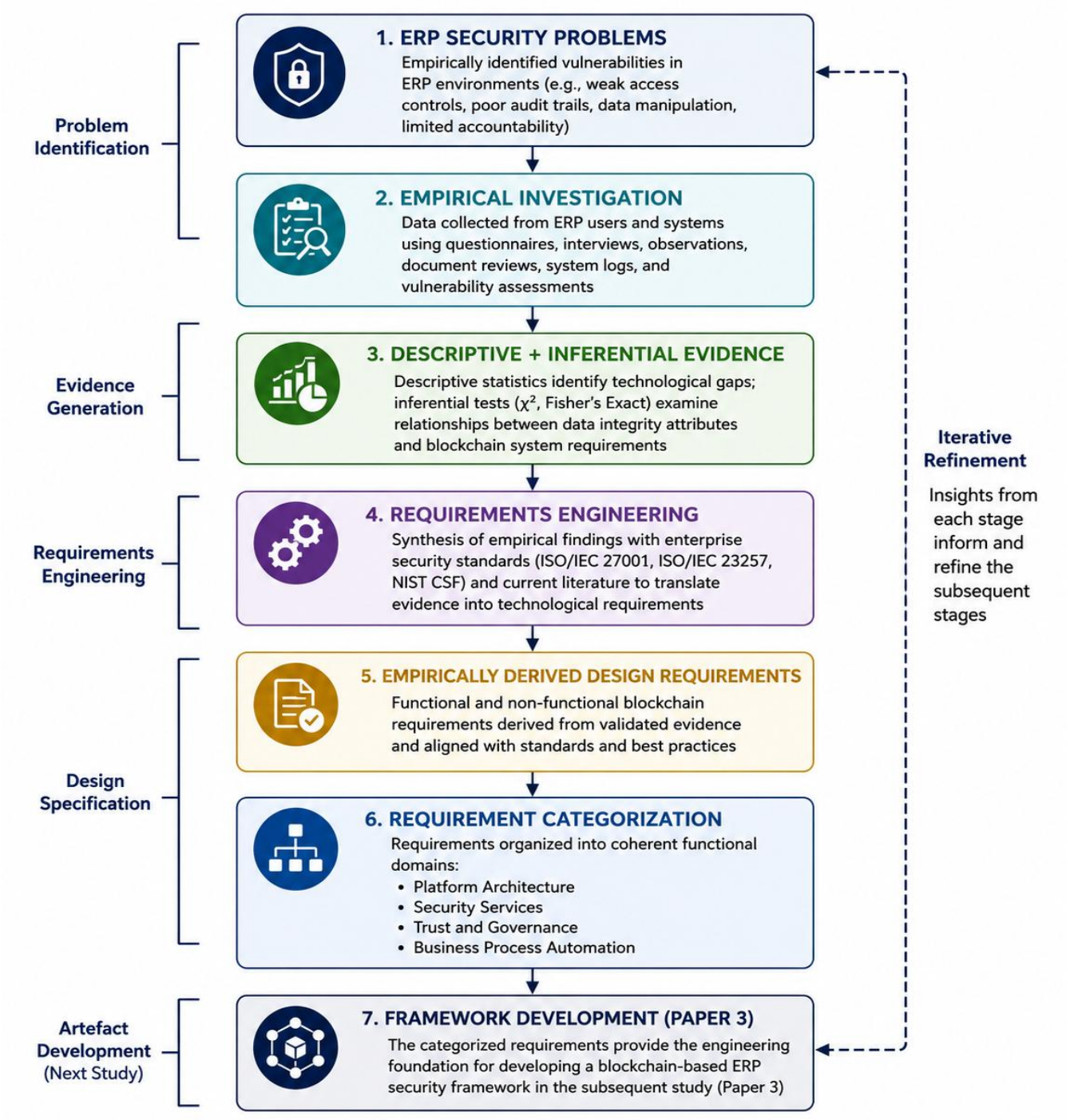
Derivation of Empirically Grounded Design Requirements

Empirical results were carefully turned into technological possibilities and the design requirements were formulated. This process incorporated three sources of evidence, namely, findings from the studies, internationally agreed upon information-security standards, and literature from the enterprise blockchain field. The standards used included ISO/IEC 27001:2022, ISO 23257:2022, the NIST Cybersecurity Framework (CSF) 2.0 and the literature related to blockchain (Casino et al., 2019; International Organization for Standardization [ISO], 2022a, 2022b; National Institute of Standards and Technology [NIST], 2024; Yue et al., 2022; Zheng et al., 2017). The evidence-based Requirements Engineering process of converting empirical findings to engineering specifications and implementable engineering design requirements are shown in Figure 2.

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

Figure 2

Evidence-based process for deriving blockchain design requirements for Enterprise Resource Planning (ERP) security within the Design Science Research paradigm.



The requirements resulting from the empirical findings are summarized in table 6, which provides a direct link between the findings and the technology gaps and design requirements.

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

Table 6

Empirically Derived Technological Design Requirements for Blockchain-Enabled Enterprise Resource Planning Systems.

Empirical finding	Technological gap identified	Design requirement
Blockchain platform readiness (28%)	Inadequate blockchain-compatible enterprise architecture	Deploy a permissioned blockchain platform integrated with the existing ERP environment.
DLT readiness (28%)	Limited distributed processing capability	Establish distributed ledger infrastructure to support distributed transaction processing.
Node infrastructure (77.8%)	Limited distributed-node capability	Strengthen node deployment, synchronization, redundancy, and network resilience.
Security control readiness (20.5%)	Limited security-control capability	Implement enhanced identity and access management with RBAC and multi-factor authentication.
Tamper-proof readiness (10.3%)	Editable transaction records and audit logs	Implement immutable ledgers, cryptographic hashing, and tamper-evident audit trails.
Transaction verification readiness (33%)	Inadequate transaction validation	Introduce distributed transaction verification supported by blockchain consensus mechanisms.
Business process automation readiness (25%)	High dependence on manual workflow execution	Implement smart contracts to automate predefined ERP business processes and policy enforcement.
Consensus readiness (38%)	Weak consensus governance	Establish formal validator governance, consensus protocols, and multi-party transaction validation.
Cryptographic readiness (12%)	Inadequate cryptographic protection and key management	Implement enterprise cryptographic services, digital signatures, and secure key management.

In order to reinforce the traceability, in the design requirements the empirical basis, supporting standards and literature, and architectural purpose were mapped.

Table 7

Traceability of empirically derived design requirements for a blockchain-based Enterprise Resource Planning security framework

Design requirement	Empirical Basis	Supporting literature/Standard	Architectural Justification
Blockchain-compatible ERP platform	Blockchain platform readiness (28.0%)	Casino et al. (2019); ISO 23257:2022	Provides the infrastructure required to integrate blockchain services with the existing ERP environment.
Distributed Ledger Technology capability	Distributed Ledger Technology readiness (28.0%)	Zheng et al. (2017); ISO 23257:2022	Provides distributed transaction recording and synchronization across participating nodes.
Enterprise node infrastructure	Node infrastructure readiness (77.8%)	ISO 23257:2022	Supports node deployment, synchronization, redundancy, and resilient communication within the distributed environment.
Identity and access management	Security control readiness (20.5%)	ISO/IEC 27001:2022; NIST CSF 2.0	Strengthens authentication, authorization, role-based access control, and user accountability.
Immutable transaction records	Tamper-proof readiness	ISO/IEC 27001:2022	Supports protection of transaction records through immutable and tamper-evident recording

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

Design requirement	Empirical Basis	Supporting literature/Standard	Architectural Justification
	(10.3%)		mechanisms.
Distributed transaction verification	Transaction verification readiness (33.0%)	Yue et al. (2022)	Supports transaction validation through distributed verification mechanisms.
Smart-contract capability	Business process automation readiness (25.0%)	Casino et al. (2019)	Supports automated execution of predefined ERP workflows and organizational business rules.
Consensus governance	Consensus readiness (38.0%)	ISO 23257:2022	Supports controlled multi-party transaction validation through defined consensus and validator governance mechanisms.
Cryptographic security services	Cryptographic readiness (12.0%)	ISO/IEC 27001:2022; NIST CSF 2.0	Supports confidentiality, integrity, authenticity, and accountability through cryptographic controls and digital signatures.

A traceability matrix for all design requirements that connects them to their empirical foundation and supporting literature and standards is included as Table 7. Tables 6 and 7 show the process and the mapping of organization weaknesses to traceable and implementable design requirements.

Categorization of the Design Requirements

The proposed framework for blockchain based ERP security was structured along four complementary domains that serves as a basis for the design requirements: Platform Architecture, Security Services, Trust and Governance, and Business Process Automation.

Table 8

Categorization of empirically derived design requirements

Requirement category	Design requirements	Primary objective
Platform Architecture	Blockchain-compatible ERP platform; Distributed Ledger Technology capability; Enterprise node infrastructure.	Provide the foundational architecture required for secure, scalable, interoperable, and resilient blockchain-enabled ERP operations.
Security Services	Identity and access management; Immutable transaction records; Cryptographic security services	Safeguard ERP assets through identity management, cryptographic protection, immutable records, and access governance.
Trust and Governance	Consensus governance; Distributed transaction verification	Support trusted transaction validation, transparency, accountability, and controlled multi-party decision-making.
Business Process Automation	Smart-contract capability	Automate ERP workflows, enforce organizational policies, reduce manual intervention, and improve operational efficiency.

The categorization can be used as a framework for the development. Platform Architecture offers the infrastructure, Security Services safeguard identities and transactions, Trust and Governance are used to ensure validated and accountable transaction processing and Business Process Automation to control the execution of predetermined ERP processes. The four domains are a core engineering basis for the proposed ERP security framework based on the blockchain technology.

Conclusion

The purpose of this study was to explore the challenges of introducing blockchain technology in Enterprise Resource Planning (ERP) systems in Public Sector Water and Sanitation (WS) organizations in Kenya. It was based on Design Science Research (DSR) to determine the readiness to integrate blockchain, explored the relationships between data-integrity attributes of ERP

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

and blockchain integration requirements, and converted the empirical results into a set of stakeholder requirements, set of engineering specifications, and set of implementable design requirements. The results revealed significant lack of readiness for blockchain integration. The readiness for blockchain platform and Distributed Ledger Technology came in at 28.0% each while readiness for security control, tamper proof, transactions verification, business process automation, consensus, and cryptographic readiness was 20.5%, 10.3%, 33.0%, 25.0%, 38.0% and 12.0% respectively. The readiness for node infrastructure and node discovery were relatively high (77.8% and 72.2%) but were still lower than the ≥90% level. The results show that current ICT infrastructure is not enough to be considered as prepared for a secure integration of blockchain in ERP. Using inferential analysis, statistically significant association was found between the cross module consistency and platform readiness ($\chi^2 = 12.042$, $p = .001$; Cramer's $V = .333$) which showed a moderate correlation. None of the other relationships tested were significant ($p > .05$). The results show that there are enterprise architecture, security, transaction verification, governance, interoperability, cryptographic protection, and business process automation requirements to implement blockchain integration beyond the scope of just technical controls. The study also proved that the identified organizational gaps were able to be systematically converted to implementable design requirements using the evidence based Requirements Engineering process. The process is from empirical evidence to technological gap and then to design requirements with technical justifications from the standards and literature, and finally to design decisions; this process is traceable. This is achieved primarily by showing how the empirically supported evidence of an organization can be systematically translated to the traceable engineering specifications and implementable design requirements in DSR. The requirements that emerge from this process give a structure to build blockchain-based ERP security solutions for transaction integrity, auditability, traceability, identity and access management, interoperability, accountability, governance and secure digital transformation.

Recommendations

From the conclusions, public-sector organizations that are looking into deploying blockchain-based ERP security should evaluate and build up technological readiness first. The blockchain platform and DLT capability, the nodes infrastructure, network resilience, and interoperability with the current ERP modules are the main areas of focus. Before technology is adopted, requirements validation and architectural assessment should be conducted to ensure implementation, rather than for the sake of better perceived benefits. Transaction and security controls must be enhanced by implementing identity and access management, role-based access control, multi factor authentication, cryptographic services, secure key management, immutable transaction records and distributed transaction verification by organizations. These controls should be in addition to existing ERP security controls and be consistent with governance and accountability requirements. Business processes should be standardized and digitized, and be able to be automated in a controlled manner and be implemented in the future with smart contracts. Governance arrangements should cover the selection of validators, management of consensus, transaction approval, security monitoring and accountability, and interoperability mechanisms should enable the consistent exchange of information between the modules in interconnected ERP systems. Implementation should follow the guidance of the recognized standards ISO/IEC 27001:2022, ISO 23257:2022 and the NIST Cybersecurity Framework (CSF) 2.0. While technology is new, investments in blockchain should be based on a solid assessment of needs and organizational capacity, and on governance planning. The proposed framework should be implemented and tested in operational environments; the effectiveness of the security, interoperability, operational performance, scalability, ease of implementation, user acceptance of the framework, and the impact on the organization should be examined. Other public-sector and critical infrastructure organizations could validate the transferability of the proposed Requirements Engineering approach.

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

Research Contribution

It offers theoretical, methodological and practical contributions to ERP security, integration of blockchain into ERP, Requirements Engineering and Design Science Research. Theoretically, the study will be an extension of the application of the Technology–Organization–Environment (TOE) framework, and will help identify the requirements for the integration of blockchain in public-sector ERP. The results reveal that readiness for integration is far more complex than simply the technological infrastructure and includes organizational capabilities, governance, interoperability, security controls, and regulatory aspects. Methodologically, the main contribution is the development of a Requirements Engineering process that incorporates quantitative and qualitative results, information from various sources within the organization, observations of the system, security requirements and blockchain literature to convert validated problems to stakeholder requirements, engineering specifications and design requirements to be implemented. Explicit engineering specification as an intermediary abstraction layer enhances traceability of the empirical investigation to the artefact design and also decouples the needs of the organization from specific technological solutions. This offers a clear, and in some cases reproducible, way of requirements-driven DSR. The study offers practical design requirements for platforms, DLT, nodes, identity and access management, immutable transaction logs, cryptographic security, distributed verification of transactions, consensus governance, and smart-contract capability. The requirements offer a foundation for security capabilities to be measured by both developers and ERP admin, security practitioners, managers, and policymakers, prior to implementing blockchain. The Requirements Engineering process also offers a methodological reference for other enterprise information systems currently going through digital transformation, establishing explicit connections between the organizational problems and the following design decisions.

Declaration Use of Generative AI

During the preparation of this manuscript, generative artificial intelligence tools were used solely to assist with language editing, grammar, clarity, and formatting. The scientific content, interpretation of findings, methodological decisions, citations, and conclusions were developed, reviewed, and verified by the authors. The authors take full responsibility for the accuracy, originality, integrity, and final content of the manuscript.

Funding:

This research received no external funding.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data supporting the findings of this study are available from the corresponding author upon reasonable request. The data are not publicly available because they contain organizational information obtained under confidentiality agreements.

Ethical Approval

Ethical approval and organizational authorization were obtained before data collection. Participation was voluntary, informed consent was obtained from all participants, and confidentiality and anonymity were maintained throughout the study.

CRediT Authorship Contribution Statement

Dennis Boera Onchwari: Conceptualization, Methodology, Investigation, Data Curation, Formal Analysis, Validation, Visualization, Writing Original Draft, Writing Review and Editing.

Lamek Ronoh: Supervision, methodology, validation, writing review and editing.

James Abila: Supervision, validation, writing review and editing.

Acknowledgements

The authors sincerely thank the management and staff of Gusii Water and Sanitation Company (GWASCO) and Kericho Water and Sanitation Company (KEWASCO) for their cooperation during data collection. The authors also acknowledge the support provided by Rongo University and appreciate the constructive comments

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

from reviewers, which greatly improved the quality of this manuscript.

References

Agresti, A. (2019). *An introduction to categorical data analysis* (3rd ed.). John Wiley & Sons.

Baker, J. (2012). The technology–organization–environment framework. In Y. K. Dwivedi, M. R. Wade, & S. L. Schneberger (Eds.), *Information systems theory: Explaining and predicting our digital society* (Vol. 1, pp. 231–245). Springer.

Braun, V., & Clarke, V. (2022). *Thematic analysis: A practical guide*. SAGE Publications.

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., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE Publications.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297–334. https://doi.org/10.1007/BF02310555

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105. https://doi.org/10.2307/25148625

International Organization for Standardization. (2022a). *ISO 23257:2022: Blockchain and distributed ledger technologies—Reference architecture*. ISO.

International Organization for Standardization. (2022b). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.

Isbaih, S., Al Noman, H., Aljarwan, A., Al Owais, I., Yosry, A., & Bahroun, Z. (2024). Blockchain in enterprise resource planning systems: A comprehensive review of emerging trends, challenges, and future perspectives. *Management Systems in Production Engineering, 32*(4), 571–586. https://doi.org/10.2478/mspe-2024-0055

Jacobs, F. R., & Weston, F. C. (2007). Enterprise resource planning (ERP)—A brief history. *Journal of Operations Management, 25*(2), 357–363.

Kothari, C. R. (2004). *Research methodology: Methods and techniques* (2nd ed.). New Age International Publishers.

Kumar, V., Gupta, S., & Singh, R. (2023). Enterprise resource planning systems and digital transformation: Emerging trends and future directions. *Journal of Enterprise Information Management, 36*(6), 1705–1728. https://doi.org/10.1108/JEIM-12-2021-0498

Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative and qualitative approaches*. ACTS Press.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Onapsis. (2021, July 2). *It's time to take the ransomware threat to business-critical SAP applications more seriously*. https://onapsis.com/blog/its-time-take-ransomware-threat-business-critical-sap-applications-more-seriously/

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Saunders, M., Lewis, P., & Thornhill, A. (2023). *Research methods for business students* (9th ed.). Pearson.

Sommerville, I. (2016). *Software engineering* (10th ed.). Pearson.

Sunmola, F., & Lawrence, G. L. (2024). Key success factors for integration of blockchain and ERP systems: A systematic literature review. *Procedia*

Received 25/08/2026; Revised 25/09/2026; Accepted 05/10/2026

Computer Science, 232, 775–782. https://doi.org/10.1016/j.procs.2024.01.077

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education, 48*(6), 1273–1296. https://doi.org/10.1007/s11165-016-9602-2

Tashakkori, A., & Teddlie, C. (2021). *The SAGE handbook of mixed methods in social & behavioral research* (3rd ed.). SAGE Publications.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

Wiegers, K., & Beatty, J. (2013). *Software requirements* (3rd ed.). Microsoft Press.

Yue, X., Ren, H., Zhang, Y., Shu, R., & Wang, J. (2022). Blockchain consensus mechanisms: A survey and classification. *Journal of Network and Computer Applications, 202*, 103353. https://doi.org/10.1016/j.jnca.2022.103353

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). *An overview of blockchain technology: Architecture, consensus, and future trends*. In *2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557–564). IEEE. https://doi.org/10.1109/BigDataCongress.2017.85