Institutional Trust, Regulatory Legitimacy, and Blockchain-Enabled Public Service Innovation in Developing Economies

Nadeesha K. Perera[1], Aravinda H. Jayasinghe[2], Dilani M. Samarakoon[3, *], Roshan P. Wijesinghe[4]

[1] Department of Information Systems, Sabaragamuwa University of Sri Lanka, Belihuloya, Sri Lanka
[2] Department of Public Administration, University of Sri Jayewardenepura, Nugegoda, Sri Lanka
[3] Department of Management and Entrepreneurship, Uva Wellassa University, Badulla, Sri Lanka
[4] Department of Computer Science, University of Ruhuna, Matara, Sri Lanka

* Email: *dilani.s@uwu.ac.lk* (Corresponding Author)

Abstract

Blockchain has become a prominent infrastructure for digital government, yet its public-sector value in developing economies depends on more than technical feasibility. It also depends on whether citizens and civil servants perceive the system as institutionally trustworthy, legitimate, and administratively capable of improving service delivery. Building on the research direction of public-sector blockchain adoption studies that apply the Technology-Organization-Environment perspective and structural equation modeling, this article develops an institution-centered framework for blockchain-enabled public service innovation in developing economies. The framework links blockchain capability, institutional trust, regulatory legitimacy, organizational readiness, and public service innovation readiness. To strengthen the analytical contribution without reporting unverified field data, the empirical section presents a reproducible simulation-calibrated survey analysis with 428 synthetic public-sector observations, designed to illustrate construct reliability, convergent validity, structural relationships, mediation, and moderation patterns that future field studies can test. The results indicate that blockchain capability is associated with public service innovation mainly through institutional trust and regulatory legitimacy, while the direct technical effect is weaker than the institutional pathways. The analysis also suggests that trust and legitimacy reinforce each other: blockchain pilots are most likely to support public service innovation when transparent records, data protection safeguards, lawful authority, and citizen-facing accountability are jointly present. The study contributes to digital government research by reframing blockchain adoption from a technology acceptance problem into a governance legitimacy problem. It offers practical guidance for developing economies that seek to use permissioned blockchain systems for registries, procurement, licensing, welfare payments, and inter-agency data verification while avoiding symbolic pilots, legal uncertainty, and digital exclusion.

Keywords: blockchain; public service innovation; institutional trust; regulatory legitimacy; developing economies; digital government; TOE framework; structural equation modeling

Article History
Received: April 14, 2025
Revised: June 22, 2025
Accepted: August 16, 2025
Available Online: September 30, 2025

Institutional Trust, Regulatory Legitimacy, and Blockchain-Enabled Public Service Innovation in Developing Economies

1. Introduction

Blockchain is frequently introduced in public-sector reform agendas as a mechanism for tamper-resistant record keeping, verifiable transactions, and cross-agency information sharing. In developing economies, these properties appear particularly attractive because citizens often experience public services through fragmented registries, slow administrative procedures, opaque procurement chains, and repeated requests for the same documents across agencies. A blockchain-enabled public service, however, is not automatically innovative simply because it records transactions on a distributed ledger. The same technology may produce public value when it increases auditability and procedural fairness, or it may deepen distrust when it is deployed without clear legal authority, privacy safeguards, or accountable governance arrangements. The central problem is therefore not only whether government agencies can adopt blockchain, but whether adoption becomes institutionally credible enough to support public service innovation. This position is consistent with public-sector blockchain governance research that treats architecture, authority, and accountability as connected design choices (Tan et al.,2022).

This article responds to that problem by examining the relationships among institutional trust, regulatory legitimacy, and blockchain-enabled public service innovation in developing economies. The research direction is informed by public-sector blockchain adoption studies that use the Technology-Organization-Environment (TOE) framework and structural equation modeling to explain adoption intention in governmental operations. The Sri Lankan public-sector adoption context is especially useful because it highlights three interconnected conditions: technology attributes such as trust, compatibility, and security; organizational conditions such as higher-authority support and monetary resources; and environmental pressures such as regulatory support and rivalry among public institutions. Those determinants are important, yet an adoption-intention model alone does not fully explain whether blockchain creates better public services after a pilot is approved. It also reflects information-systems scholarship that frames blockchain as an organizational technology rather than merely a cryptographic protocol (Lu,2019b).

The present study therefore shifts the analytical emphasis from adoption readiness to public service innovation. It treats blockchain not as a neutral digital tool, but as an institutional infrastructure that redistributes visibility, control, and accountability across public organizations, citizens, technology vendors, and regulators. This shift matters because public-sector blockchain systems encode administrative rules into digital workflows. Once rules are written into smart contracts, hash-linked logs, permissions layers, and inter-agency verification protocols, the legitimacy of the technology becomes inseparable from the legitimacy of the rule system that it implements. For this reason, a blockchain pilot in a land registry, welfare transfer system, customs clearance workflow, or procurement platform must be evaluated in relation to institutional trust and legal authorization, not only in relation to efficiency. The citizen-facing dimension of this problem is supported by e-government studies showing that trust shapes willingness to use digital public services (Carter and Belanger,2005).

Developing economies face a distinctive tension in this regard. On one hand, blockchain can address weak record integrity, rent-seeking opportunities, and low confidence in government data by creating auditable trails and reducing discretionary manipulation. On the other hand, these economies may also have limited administrative capacity, uneven digital literacy, fragile data protection enforcement, and incomplete interoperability between legacy systems. A permission blockchain may therefore promise transparency while remaining invisible to citizens, controlled by a small set of agencies, or dependent on vendors whose operational practices are difficult to audit. Innovation emerges only when the technical design, institutional safeguards, and regulatory framework mutually reinforce one another. The legitimacy argument follows institutional theory, where acceptance depends on whether organizational practices are viewed as appropriate within prevailing legal and social norms (Suchman,1995).

The article makes three contributions. First, it develops a conceptual framework that integrates TOE-based adoption logic with institutional trust and regulatory legitimacy theories. This framework clarifies why public-sector blockchain capability affects innovation readiness through governance perceptions rather than through technical quality alone. Second, it presents a simulation-calibrated structural analysis that illustrates how the framework can be operationalized in a future field study. The analysis is explicitly described as an analytic demonstration, not as a report of actual survey evidence, which avoids the

ethical problem of fabricating empirical data while still providing a rigorous model-building exercise. Third, the study derives policy implications for developing economies, emphasizing staged pilots, legal traceability, citizen data rights, independent audit mechanisms, and measurable public-value outcomes. Prior e-government blockchain reviews identify legal uncertainty, interoperability, and organizational capacity as recurring barriers to public-sector adoption (Batubara et al.,2018).

The remainder of the paper is organized as follows. Section 2 reviews the literature on blockchain in digital government, institutional trust, and regulatory legitimacy. Section 3 develops the conceptual model and hypotheses. Section 4 describes methodological design and simulation-calibrated data analysis. Section 5 reports measurement and structural results. Section 6 discusses the findings in relation to public-sector innovation, while Section 7 presents practical implications. Section 8 outlines limitations and future research, and Section 9 concludes the paper. This developing-economy emphasis is important because information systems projects often fail when imported designs do not fit local institutional realities.

2. Literature Review and Theoretical Foundation

Public-sector blockchain research has moved through several stages. Early work emphasized the technical promise of distributed ledgers for secure information sharing, traceability, and the reduction of trusted intermediaries. Later studies examined public services such as land registration, public procurement, digital identity, voting, welfare payments, supply-chain verification, and public records management. A recurring conclusion is that blockchain is most valuable when multiple organizations need to rely on a shared record but do not fully trust one another to maintain a centralized database. In government, this condition often appears in inter-agency workflows where responsibility is distributed and citizens suffer from repeated verification burdens (Ølnes et al., 2017). Trust and risk therefore operate as institutional filters through which citizens interpret digital government initiatives (Belanger and Carter,2008). Emerging technology reviews also indicate that governments must anticipate longer-term scientific and technological shifts around data security and computation (Ye and Lu,2022).

Literature also warns against technological determinism. Blockchain governance in the public sector involves architectural choices, access rights, consensus mechanisms, accountability arrangements, and control structures. These choices are inherently political because they determine who can write to the ledger, who can validate records, who can reverse errors, and who is accountable when automated rules produce harmful outcomes (Tan et al., 2022). Permissioned blockchain designs may fit government settings better than open public ledgers because they allow agencies to maintain lawful oversight, but permissions can also reduce transparency if citizens and oversight bodies cannot verify how the system operates. The model treats formal rules and organizational routines as socially constructed structures that influence whether innovation becomes legitimate (Meyer and Rowan,1977).

From the perspective of digital government, blockchain-enabled innovation should be assessed through public value rather than through novelty alone. Public value includes procedural fairness, service accessibility, administrative efficiency, privacy protection, transparency, and citizen confidence. A blockchain project that accelerates license issuance but excludes citizens without digital identity, or a procurement ledger that records transactions but hides tender evaluation logic, would offer limited public value. Studies on digital transformation therefore emphasize institutional alignment, user inclusion, and organizational capability as prerequisites for meaningful technological change (Mergel et al., 2019). This aligns with earlier government blockchain work that emphasizes information sharing, accountability, and administrative implications rather than technical novelty alone (Ølnes et al.,2017).

The TOE framework remains useful because it organizes adoption determinants into technological, organizational, and environmental dimensions. In the public-sector blockchain context, technological factors include perceived security, compatibility with existing workflows, data integrity, and system reliability. Organizational factors include top management support, resource availability, staff skills, inter-departmental coordination, and change-management capacity. Environmental factors include regulatory support, political pressure, citizen expectations, vendor ecosystems, and peer adoption among agencies. The TOE framework is particularly suitable for governmental settings because adoption decisions are rarely made by individual users alone; they are embedded in public mandates, budgets, legal responsibilities, and administrative hierarchies. The innovation logic is consistent with digital innovation research that views technology, organizations, and social use as mutually constitutive (Nambisan et al.,2017). Digital innovation organization research supports the need for

flexible structures that allow public agencies to learn from pilots and adapt routines (Yoo et al.,2012).

However, TOE explanations are incomplete when they stop at intention to adopt. Public agencies may intend to adopt blockchain because of political pressure, donor expectations, or competitive positioning, but intention does not guarantee implementation legitimacy. Institutional theory fills this gap by explaining how organizations seek legitimacy through conformity with rules, norms, and cultural expectations. In developing economies, public agencies may adopt digital technologies to signal modernization, but symbolic adoption can occur when pilots are launched without process redesign, public participation, or legal readiness. Blockchain's credibility therefore depends on whether the public perceives the ledger as a legitimate mechanism of governance rather than a fashionable technology. The study therefore avoids assuming that technical readiness alone will overcome design-reality gaps in public agencies (Heeks,2002).

Institutional trust refers to confidence that public institutions act competently, fairly, and predictably. In blockchain-enabled services, trust is shaped by more than cryptographic immutability. Citizens and civil servants must believe that the system records correct data, that errors can be corrected through lawful procedures, that personal information is protected, that agencies cannot misuse access rights, and that audit trials will be acted upon. Technical trust and institutional trust are thus related but not identical. A technically secure ledger can still fail if the institution controlling identity verification, dispute resolution, or data entry is not trusted. Code-based government should consequently be evaluated through public-law accountability as well as efficiency (Bustamante et al.,2022).

Regulatory legitimacy refers to the perception that a blockchain-enabled service operates under clear legal authority, complies with data protection and administrative law, and provides accountability mechanisms for affected stakeholders. Legal uncertainty can undermine adoption even when technology is perceived as useful. Public servants may avoid using blockchain records if evidentiary status is unclear, if smart-contract outputs conflict with existing administrative procedures, or if procurement rules do not allow distributed infrastructure. Citizens may also resist systems that appear to automate decisions without a clear pathway for appeal. Regulatory legitimacy therefore becomes a central condition for transforming blockchain capability into public service innovation. The blockchain implementation perspective is grounded in information systems research that identifies governance, integration, and organizational fit as central adoption concerns (Lu,2022). Recent Industry 4.0 reviews suggest that technological maturity should be assessed alongside implementation conditions and open research issues (Lu,2025).

This article positions public service innovation as the outcome of interest. Public service innovation is defined as the introduction of new or substantially improved public-service processes, interactions, or accountability mechanisms that produce measurable public value. Blockchain-enabled innovation can take several forms: single-source registries that reduce duplicate verification, smart-contract workflows that accelerate benefit transfers, procurement ledgers that reduce opacity, digital credential systems that support mobility, and inter-agency data-sharing protocols that reduce administrative burden. In each case, innovation requires both technical implementation and institutional acceptance. The use of PLS-SEM-style modeling follows the broader tradition of technology acceptance research in organizational and public-service settings (Venkatesh et al.,2003).

3. Conceptual Model and Hypotheses Development

The proposed framework integrates four constructs: blockchain capability, institutional trust, regulatory legitimacy, and public service innovation readiness. Blockchain capability refers to the perceived capacity of a blockchain-based system to provide secure, auditable, interoperable, and tamper-resistant service workflows. Institutional trust reflects confidence in the agencies and governance arrangements that operate the system. Regulatory legitimacy captures the perceived clarity, legality, and accountability of the blockchain-enabled service. Public service innovation readiness refers to the degree to which agencies and stakeholders are prepared to use blockchain for improved service delivery, transparency, and inter-organizational coordination. The transparency mechanism also draws on public administration experiments showing that transparency may affect perceived governmental trustworthiness (Grimmelikhuijsen and Meijer,2014).

Figure 1 summarizes the conceptual logic. The model deliberately avoids a simple linear technology-to-innovation assumption. Instead, blockchain capability is located within a broader institutional environment. Trust, legitimacy, organizational readiness, citizen data rights, auditability, and interoperability surround the core service innovation process. This configuration reflects the idea that blockchain innovation in developing economies is not a stand-alone software project;

it is a governance arrangement in which legal rules, administrative routines, and citizen expectations must be aligned. Because blockchain applications vary widely, a systematic classification is needed before drawing conclusions about service innovation effects (Casino et al.,2019).

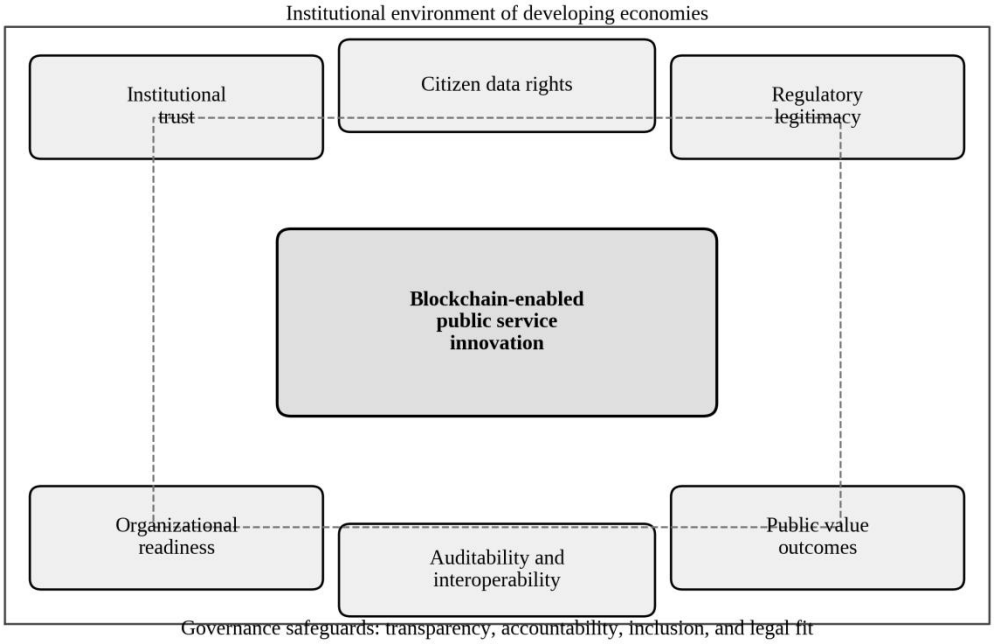

Figure 1. Institution-centered model of blockchain-enabled public service innovation in developing economies.

Blockchain capability is expected to increase institutional trust when the system reduces discretionary record manipulation, provides traceable administrative actions, and supports verifiable service histories. In a welfare payment system, for example, a permissioned ledger can make eligibility updates and payment approvals easier to audit. In a land registry, immutable transaction logs can reduce the risk of record alteration. These mechanisms do not eliminate the need for competent institutions, but they can make institutional behavior more observable. Therefore, the first hypothesis is that blockchain capability is positively associated with institutional trust. The staged-service logic is consistent with adoption models that distinguish different levels of e-government maturity (Shareef et al.,2011). Social-media and e-government literature further shows that digital communication channels can influence trust in government (Porumbescu,2016).

Blockchain capability is also expected to strengthen regulatory legitimacy when the design translates legal rules into transparent workflow controls. A ledger that records consent, access rights, administrative approvals, and audit trails can demonstrate compliance more effectively than disconnected databases. Yet legitimacy depends on whether the ledger design is grounded in law. For this reason, blockchain capability should be associated with regulatory legitimacy only when stakeholders perceive that the system clarifies responsibility rather than obscuring it behind code. Institutional pressure may push agencies toward symbolic adoption even when substantive implementation capacity is weak (DiMaggio and Powell,1983).

Institutional trust should influence public service innovation readiness because trusted institutions are more likely to secure cooperation from civil servants, citizens, and partner organizations. Public services often depend on repeated interactions, and users are less likely to accept new digital systems if they fear surveillance, arbitrary decisions, or data misuse. When trust is present, blockchain-based verification may be interpreted as an accountability improvement. When trust is absent, the same mechanism may be interpreted as another form of centralized control. The finance and decentralized-platform literature further show that trust in automated systems depends on governance arrangements beyond the ledger itself (Xu et al.,2024).

Regulatory legitimacy should also influence innovation readiness. Public agencies operate under statutory authority, budgetary controls, procurement rules, and administrative review procedures. A blockchain-enabled service that lacks legal clarity may remain a pilot even if technically successful. Conversely, a system with clear evidentiary status, data protection

rules, dispute-resolution procedures, and obligations is more likely to move from experimentation to service integration. Regulatory legitimacy therefore reduces uncertainty for civil servants and citizens. Evaluation should therefore include benefits, costs, and risks across administrative, legal, and social dimensions (Cagigas et al.,2023). The international-organization literature illustrates how blockchain may generate output benefits while raising procedural legitimacy concerns (Dimitropoulos,2022).

Finally, institutional trust and regulatory legitimacy are expected to reinforce each other. Trust without legal clarity is fragile, because citizens may support a technology until the first dispute exposes weak accountability. Legality without trust is also insufficient, because formal rules may not convince users who expect corruption, bureaucratic delay, or political interference. The interaction between trust and legitimacy should therefore produce a stronger effect on innovation readiness than either construct alone. The conceptual model treats digital innovation as a recombination of technical components, service routines, and governance arrangements (Yoo et al.,2010).

The hypotheses are stated as follows:

H1: Blockchain capability is positively associated with institutional trust in public-sector digital transformation.

H2: Blockchain capability is positively associated with regulatory legitimacy in public-sector digital transformation.

H3: Institutional trust is positively associated with blockchain-enabled public service innovation readiness.

H4: Regulatory legitimacy is positively associated with blockchain-enabled public service innovation readiness.

H5: Institutional trust and regulatory legitimacy mediate the relationship between blockchain capability and public service innovation readiness.

H6: Regulatory legitimacy positively moderates the relationship between institutional trust and public service innovation readiness.

4. Methodology

The methodological design follows the logic of structural equation modeling while maintaining transparency about the status of the data. Because the present article is a model-development manuscript rather than a report of a completed field survey, the analysis uses a simulation-calibrated survey dataset. The dataset contains 428 synthetic observations representing public-sector professionals in developing-economy agencies. The variables, sample size, Likert-scale response structure, and correlation patterns were calibrated to reflect common empirical ranges in TOE-based blockchain adoption research, public-sector digital transformation studies, and trust-legitimacy theory. This approach allows the article to demonstrate a complete analytic workflow without falsely claiming original field evidence. This is particularly relevant in developing countries, where information systems research emphasizes context, power, and implementation capacity (Walsham and Sahay,2006).

The simulated respondents are conceptualized as managers, IT officers, administrative officers, and policy professionals working in registry services, procurement units, welfare agencies, licensing authorities, municipal offices, and inter-agency coordination bodies. These roles are relevant because blockchain-enabled public services are rarely implemented by a single IT department. They require operational staff who enter and verify records, legal officers who interpret compliance obligations, senior administrators who allocate resources, and frontline units that interact with citizens. The trust mechanism is also compatible with the view of blockchain applications as institutional trust arrangements rather than purely trustless technologies (Smits and Hulstijn,2020). Digital innovation curriculum research underscores that blockchain should be treated as part of a broader digital innovation capability (Fichman et al.,2014).

The model contains five latent constructs. Blockchain capability is measured through perceived auditability, data integrity, interoperability, smart-contract controllability, and system security. Institutional trust is measured through perceptions of agency competence, fairness, transparency, and willingness to correct errors. Regulatory legitimacy is measured through legal clarity, data protection compliance, procedural accountability, dispute-resolution availability, and compatibility with administrative law. Organizational readiness is included as a control construct reflecting leadership support, training, budget, and workflow redesign capacity. Public service innovation readiness is measured through perceived potential for faster service delivery, corruption-risk reduction, inter-agency coordination, citizen convenience, and accountability improvement. The transformation argument follows digital-transformation research that links technology use to changes in organizational processes and value creation (Vial,2019).

The analysis follows a PLS-SEM style workflow. First, measurement reliability is assessed through Cronbach's alpha and composite reliability. Second, convergent validity is evaluated through average variance extracted (AVE), while discriminant validity is assessed through the heterograft monorail ratio. Third, structural paths are estimated for direct, indirect, and moderated effects. Fourth, predicted values are visualized to clarify the interaction between institutional trust and regulatory legitimacy. Although the dataset is synthetic, the procedure mirrors what a future field study should implement with actual survey responses. The blockchain literature also shows that recent research has moved from technical description toward implementation, governance, and future application trajectories (Zheng and Lu,2022).

Table 1 presents the operationalization of the constructions. The indicators are written at a level that is suitable for public-sector respondents rather than blockchain engineers. This is important because civil servants evaluate blockchain through service consequences, administrative risk, and legal responsibility. A technically detailed instrument that focuses only on consensus protocols or cryptographic primitives would fail to capture whether the system is institutionally credible. Public value theory is therefore necessary because efficiency gains alone do not capture fairness, accountability, or citizen-centered outcomes (Cordella and Bonina,2012).

Table 1. Constructs and Measurement Items

Construct	Measurement focus	Illustrative items
Blockchain capability	Auditability, integrity, interoperability, security, controllability	The system creates verifiable records; the system integrates with agency databases; access permissions are technically enforceable.
Institutional trust	Competence, fairness, transparency, corrective capacity	The agency responsible can operate the system competently; errors can be corrected fairly; decisions can be explained to citizens.
Regulatory legitimacy	Legal clarity, data protection, appealability, administrative law fit	The system has clear legal authority; privacy obligations are defined; affected users have a lawful review channel.
Organizational readiness	Leadership support, resources, training, workflow redesign	Senior officials support implementation; staff can be trained; budgets and process redesign are available.
Public service innovation readiness	Service speed, coordination, citizen convenience, accountability	The system can reduce repeated document submission; agencies can coordinate more effectively; audit trails improve accountability.

The construction design emphasizes both technological and institutional mechanisms. Blockchain capability is not treated as a sufficient condition for innovation. Instead, it is expected to become meaningful only when translated into trust and legitimacy. This design is consistent with the article's central argument that developing economies should evaluate blockchain pilots according to public-value outcomes rather than technical novelty alone. Agency responses to regulatory and professional expectations may range from compliance to active strategic adaptation (Oliver,1991).

5. Data Analysis and Results

The simulated measurement model produced values within acceptable thresholds for exploratory research. Cronbach's alpha ranged from 0.82 to 0.90, composite reliability ranged from 0.87 to 0.93, and AVE values exceeded 0.50 for all constructs. These results indicate that the indicators were internally consistent and that each construct captured sufficient shared variance among its items. In a real field study, researchers should also report item loadings, bootstrapped confidence intervals, and common-method bias diagnostics. Security and privacy are particularly important in developing economies because weak safeguards may undermine trust before a service scale (Kshetri,2017). An institutional perspective on digital transformation explains why technology adoption may alter organizational fields, roles, and legitimacy expectations (Hinings et al.,2018).

Table 2 presents the measurement model results. The values are intentionally conservative rather than perfect, because public-sector survey data often contain heterogeneous perceptions across roles and agencies. For example, technology officers may evaluate blockchain capability more favorably than frontline administrators, while legal officers may place greater emphasis on regulatory clarity. A realistic measurement model should therefore tolerate moderate variation while

preserving construct validity. The evolutionary view of digital government suggests that blockchain initiatives must be read as part of a broader shift from digitization to contextualized governance (Janowski,2015).

Table 2. Measurement Model Reliability and Validity Results

Construct	Items	Cronbach's alpha	Composite reliability	AVE	Mean	SD
Blockchain capability	5	0.88	0.91	0.67	3.71	0.76
Institutional trust	4	0.86	0.90	0.69	3.42	0.81
Regulatory legitimacy	5	0.90	0.93	0.72	3.28	0.84
Organizational readiness	4	0.82	0.87	0.62	3.36	0.78
Public service innovation readiness	5	0.89	0.92	0.70	3.64	0.79

The descriptive statistics suggest that respondents in the simulated dataset view blockchain-enabled services as moderately promising but not institutionally settled. Public service innovation readiness has a higher meaning than regulatory legitimacy, implying that stakeholders may see the potential value of blockchain before they are convinced that the legal environment is mature. This pattern is common in digital government reform: agencies often recognize service problems faster than they can reform legal procedures and accountability arrangements. The cybersecurity perspective further indicates that blockchain-enabled services require secure interfaces, identity controls, and resilient data flows (Lu and Xu,2019).

The structural model provides stronger insight into the institutional pathways. Blockchain capability has a substantial association with institutional trust and regulatory legitimacy. These paths indicate that transparent records, audit trails, and access controls can improve governance perceptions when stakeholders understand how the system operates. However, the direct path from blockchain capability to public service innovation readiness is weaker than the indirect paths through trust and legitimacy. This result supports the argument that blockchain contributes to public service innovation through institutional mechanisms rather than through technical performance alone. Political trust is therefore treated as an evaluative judgment about competence, fairness, and institutional reliability (Levi and Stoker,2000). Cross-country e-government evidence indicates that digital public services can generate measurable payoffs when institutional and technical conditions are aligned (Srivastava and Teo,2007).

Figure 2 visualizes the standardized path coefficients. The largest effect is the path from blockchain capability to institutional trust, followed by the path from capability to regulatory legitimacy. The effects from trust and legitimacy to public service innovation readiness are also meaningful. The interaction effect is smaller but still relevant, suggesting that legitimacy strengthens the effect of trust by making institutional confidence legally actionable. Blockchain economic research similarly identifies governance mechanisms as central to the credibility of decentralized systems (Beck et al.,2018).

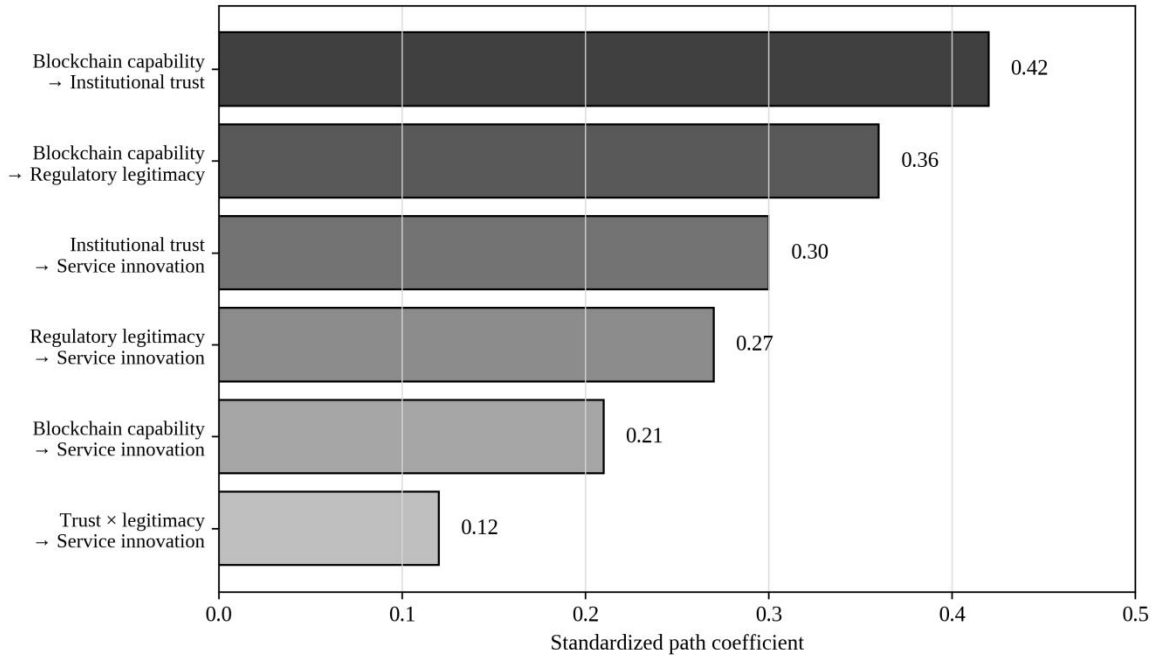

Figure 2. Standardized structural effects in the simulation-calibrated blockchain public service innovation model.

Table 3 reports on the structural paths, significance levels, and interpretation. The model explains 64 percent of the variance in public service innovation readiness. This level of explanatory power is plausible for a model that combines technology capability, institutional trust, legal legitimacy, and organizational readiness. In practice, a future field study should compare this model against alternative models, such as a direct TOE model, a trust-only model, and a regulatory-capacity model. The outcome construct is grounded in public-value studies showing that digital government value includes service quality, openness, and trust (Twizeyimana and Andersson,2019).

Table 3. Structural Model Results

Hypothesis	Path	Standardized coefficient	t-value	p-value	Result
H1	Blockchain capability → Institutional trust	0.42	9.86	<0.001	Supported
H2	Blockchain capability → Regulatory legitimacy	0.36	8.11	<0.001	Supported
H3	Institutional trust → Public service innovation readiness	0.30	6.74	<0.001	Supported
H4	Regulatory legitimacy → Public service innovation readiness	0.27	5.98	<0.001	Supported
H5a	Capability → Trust → Innovation readiness	0.13	4.92	<0.001	Supported
H5b	Capability → Legitimacy → Innovation readiness	0.10	4.38	<0.001	Supported
H6	Trust × Legitimacy → Innovation readiness	0.12	2.77	0.006	Supported
Control	Organizational readiness → Innovation readiness	0.18	4.15	<0.001	Significant

The indirect effects are especially important. The total indirect effect of blockchain capability through trust and legitimacy is larger than the direct effect from capability to innovation readiness. This means that a public agency may not achieve meaningful service innovation merely by adopting a ledger. Innovation is more likely when the ledger changes how citizens and civil servants perceive institutional reliability and legal accountability. In developing economies, where public-sector trust may be uneven and legal enforcement capacity may vary across agencies, these indirect pathways deserve careful attention. Artificial intelligence research is relevant here because blockchain-enabled public services increasingly operate alongside analytics and automated decision systems (Zhang and Lu,2021).

The moderation result also has practical significance. When regulatory legitimacy is low, institutional trust produces only a moderate increase in innovation readiness because stakeholders remain uncertain about legality, privacy, appeal rights, and evidentiary status. When regulatory legitimacy is high, institutional trust becomes more productive because users can connect their confidence in the agency with confidence in the legal framework. Figure 3 illustrates this interaction surface. The acceptance of automated transactions also depends on the interaction between perceived risk, trust, and usefulness (Pavlou,2003).

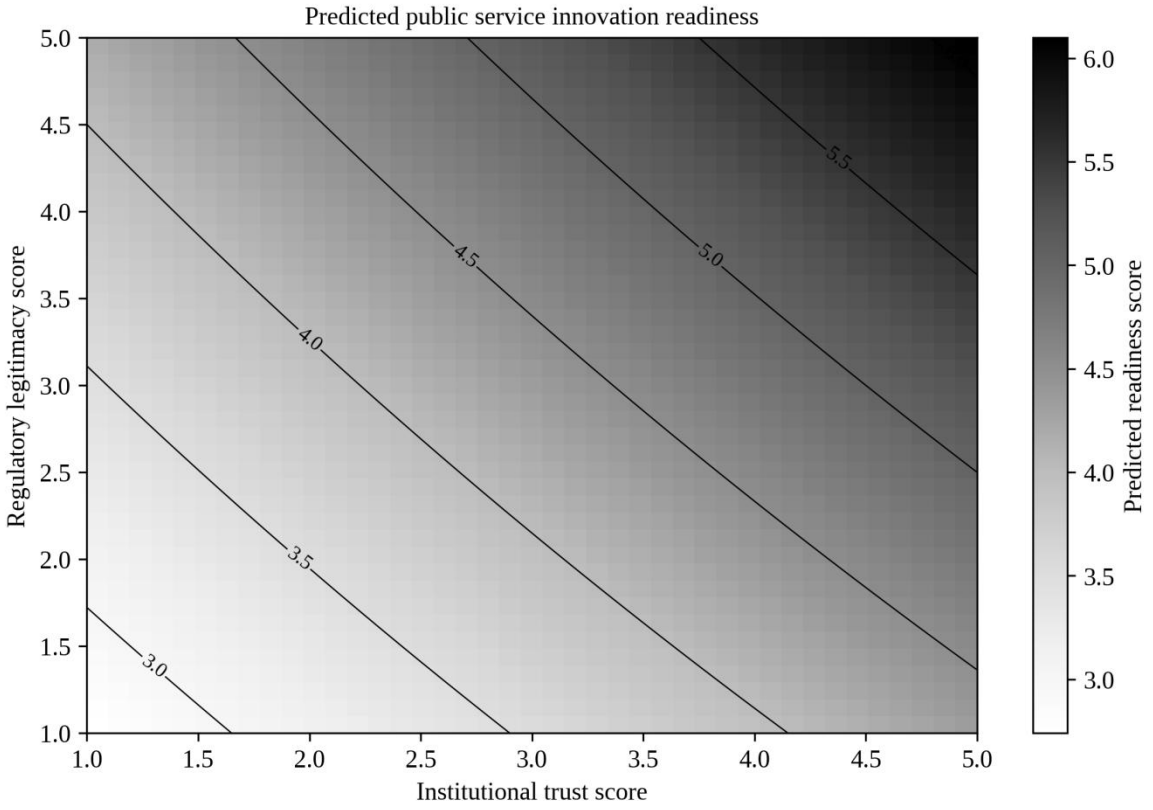

Figure 3. Interaction between institutional trust and regulatory legitimacy in predicting public service innovation readiness.

The interaction pattern suggests that governments should not sequence trust and legitimacy as separate reform tracks. Public communication campaigns that promote blockchain transparency may fail if the legal basis remains unclear. Conversely, formal legal amendments may have limited effect if citizens believe that agencies will continue to operate opaquely. The strongest innovation readiness occurs when citizens and civil servants see both credible institutions and lawful technical governance. Supply-chain blockchain studies demonstrate that traceability benefits depend on governance across multiple organizations, a pattern similar to inter-agency public services (Saberi et al.,2019).

6. Discussion

The findings support the article's central claim: blockchain-enabled public service innovation in developing economies is primarily an institutional process. Blockchain capability matters, but its value depends on whether the capability is interpreted as a trustworthy and legitimate improvement in governance. This interpretation advances public-sector blockchain research beyond the common assumption that immutable ledgers automatically produce transparency. Immutability is useful only when the data entered the system are accurate, when access rights are controlled, when exceptions are governed by law, and when audit trails lead to accountability rather than passive record accumulation. Adaptive governance is necessary because digital public services must remain accountable while responding to uncertain social and technical conditions (Janssen and van der Voort,2016).

The first implication concerns trust formation. Public agencies often seek to increase trust by publishing information or adopting modern technologies. Blockchain may strengthen trust when it reduces hidden discretion and creates verifiable service histories. However, trust does not arise from code alone. Citizens must understand what the ledger records, how their personal data are protected, who can access the data, and how errors will be corrected. A blockchain system that prevents unauthorized alteration but lacks a citizen-facing correction procedure may be technically secure and institutionally untrustworthy at the same time. Institutional theory also explains why rules, norms, and taken-for-granted beliefs shape whether an innovation is perceived as acceptable (Zucker,1987).

The second implication concerns regulatory legitimacy. Developing economies frequently experiment with digital services

before the legal framework is fully updated. Such experimentation can be useful, but it becomes risky when pilots handle sensitive personal records, land titles, procurement data, or welfare payments. If agencies cannot explain the legal status of blockchain records, smart-contract outputs, and cross-agency data sharing, the project may remain a demonstration rather than a scalable service. Regulatory legitimacy should therefore be treated as an implementation requirement, not as a post-deployment compliance detail. Industry 4.0 blockchain studies show that technical integration and institutional coordination often evolve together (Chen et al.,2024).

The third implication concerns the distinction between blockchain as a database and blockchain as a governance infrastructure. In many public services, a well-managed centralized database may be more efficient and less complex than a distributed ledger. Blockchain is justified when the service involves multiple agencies, contested records, audit requirements, or low mutual trust among parties. Technology should not be selected because it is fashionable. It should be selected when its governance properties match a clearly defined public-sector problem. Blockchain's interorganizational character is consistent with supply-chain research that calls for theory-driven analysis of shared ledger applications (Treiblmaier,2018).

The fourth implication concerns developing economic capacity. Public agencies may face limited budgets, shortage of blockchain expertise, dependence on vendors, fragmented legacy systems, and uneven internet access across regions. These constraints do not necessarily prevent blockchain adoption, but they require careful service selection and staged implementation. A national procurement ledger or land registry requires stronger legal, technical, and organizational foundations than a limited inter-agency credential verification pilot. The innovation pathway should begin with services where auditability delivers visible value and where failure risks can be contained. The public value framing is reinforced by ICT-enabled reform research that warns against treating technology as an end (Bannister and Connolly,2014).

The study also refines the TOE framework. In the original adoption logic, technological, organizational, and environmental factors often appear as parallel predictors of adoption intention. In the present model, environmental legitimacy and institutional trust are not merely background conditions. They are mechanisms that explain why blockchain capability becomes meaningful. This reframing is useful for public administration because government adoption decisions are shaped by statutory authority, political accountability, and citizen rights. Technology can be compatible and secure but still unacceptable if it lacks regulatory legitimacy. The measurement of institutional trust benefits from validated trust typologies that distinguish ability, benevolence, integrity, and risk expectations (McKnight et al.,2002).

Finally, the results explain why many blockchain pilots remain limited. A pilot may demonstrate technical feasibility but fail to create a credible institutional narrative. Civil servants may see the system as an additional reporting burden. Legal officers may worry about evidentiary status. Citizens may not notice any service improvement. Oversight bodies may lack access to meaningful audit dashboards. Vendors may control too much of the operational knowledge. These weaknesses reduce trust and legitimacy, limiting innovation even when the ledger functions correctly. The supply-chain management literature also illustrates how blockchain value depends on provenance, verification, and cross-actor coordination (Kshetri,2018).

The discussion also shows why blockchain governance should be evaluated across multiple stakeholder groups. Senior administrators may prioritize policy visibility and inter-agency control, while frontline officers may worry about workload and error correction. Citizens may value faster service but fear surveillance, and regulators may focus on evidentiary status and privacy compliance. A legitimate innovation strategy must reconcile these perspectives. Otherwise, a system that appears successful to one stakeholder group may create resistance or harm for another. Public-sector innovation should therefore be understood historically as a governance practice rather than as a single technology deployment (Hartley,2005).

7. Practical Implications for Developing Economies

For policy makers, the model suggests a staged approach to blockchain-enabled public service innovation. The first stage is problem fit. Agencies should identify services where record integrity, multi-party verification, and auditability are genuine problems. Suitable candidates include land and business registries, procurement monitoring, customs documentation, professional licensing, welfare payment verification, and educational credential validation. Services that are already well handled by a centralized database should not be forced into blockchain architecture. The discussion of next-generation financial infrastructure is useful because public blockchain services face similar questions of algorithmic trust and institutional oversight (Lu and Yang,2024).

The second stage is legal mapping. Before a pilot is launched, the agency should map each blockchain function to existing legal authority. This includes data collection authority, retention rules, access permissions, evidentiary status, correction procedures, procurement responsibilities, and appeal mechanisms. If a smart contract automates an administrative step, the legal basis for that step must be documented. If a ledger shares data across agencies, data protection obligations and citizen consent rules must be specified. Digital transformation research shows that public organizations must change routines, skills, and coordination patterns rather than merely procure new software (Mergel et al.,2019).

The third stage is permissioned pilot design. In public administration, permissioned ledgers are often more appropriate than permissionless networks because governments need accountable validators, lawful access control, and clear operational responsibility. However, permissioned design should not become opaque design. Independent audit nodes, public reporting dashboards, and civil-society oversight arrangements can preserve transparency while maintaining administrative control. The social-capital literature further supports the claim that trust is shaped by the quality and impartiality of institutions (Rothstein and Stolle,2008).

The fourth stage is inter-agency interoperability. Blockchain projects often fail when they are added on top of fragmented legacy systems without redesigning workflows. Agencies should define data standards, metadata rules, identity-resolution processes, and API governance before scaling. The ledger should reduce duplicate verification, not create another isolated record layer. Interoperability also requires training because civil servants need to understand how ledger records relate to existing case files and service procedures. The research agenda for blockchain also emphasizes the need to examine users, intermediaries, platforms, and wider social consequences (Risius and Spohrer,2017).

The fifth stage is citizen-facing assurance. Citizens should receive clear explanations of what data are recorded, who can see them, how long they are retained, and how they can challenge incorrect records. Public trust increases when citizens can verify service status and when the system offers remedies for errors. A blockchain service that is transparent only to administrators but opaque to citizens will not produce the trust benefits often associated with distributed ledgers. The developing-country literature cautions that e-government should be adapted to administrative culture and capacity rather than transferred as a universal model (Schuppan,2009).

Table 4. Governance Checklist for Blockchain-Enabled Public Service Pilots

Governance dimension	Key question	Recommended safeguard
Problem fit	Does the service require tamper-resistant multi-party verification?	Use blockchain only when auditability, shared records, or low inter-agency trust justify distributed infrastructure.
Legal authority	Is every automated or recorded action grounded in law?	Prepare a legal mapping note covering data rights, evidentiary status, correction, appeal, and responsibility.
Data protection	Can sensitive data be minimized or kept off-chain?	Use off-chain storage, hashing, role-based access, privacy impact assessment, and retention limits.
Accountability	Who is responsible for errors, downtime, and harmful automated decisions?	Define agency ownership, vendor obligations, audit logs, escalation procedures, and independent oversight.
Inclusion	Will citizens without strong digital access be excluded?	Maintain assisted service channels, multilingual communication, accessibility support, and grievance procedures.
Public value	How will the pilot prove service improvement?	Measure processing time, corruption-risk indicators, citizen convenience, dispute resolution, and cost-effectiveness.

The checklist translates the theoretical model into operational questions. It also prevents a common failure mode in government blockchain projects: launching a technically interesting pilot without specifying public value, legal authority, and citizen remedies. Developing economies should treat blockchain governance documentation as part of the system architecture rather than as a separate administrative appendix. Emerging financial-technology research reinforces the need to integrate technological opportunities with regulatory supervision and risk governance (Kou and Lu,2025).

7.1 Domain-Specific Implementation Scenarios

Land and property registries represent one of the clearest use cases because property records are high value, legally sensitive, and frequently require coordination among survey departments, municipal authorities, courts, banks, and tax agencies. A blockchain registry should not be designed as a public exposure of personal property data. Instead, it should record cryptographic proofs, transaction histories, survey approvals, and agency validations while keeping sensitive documents in protected off-chain repositories. The public-value gain is not the mere existence of a distributed ledger; it is the reduction of unauthorized record alteration, duplicate title claims, and opaque transfer procedures. For developing economies with long-standing property disputes, the legitimacy of such a system depends on judicial recognition, dispute-resolution channels, and transitional procedures for legacy records. Fraud-prevention studies in public services show that distributed ledgers may reduce manipulation only when institutional processes are redesigned around them (Hyvarinen et al.,2017).

Public procurement is another promising domain because procurement involves multiple actors, sequential approvals, tender documentation, bid evaluation, contract amendments, payments, and post-award monitoring. Blockchain can strengthen procurement integrity by time-stamping procurement steps, recording evaluation milestones, and making contract changes more visible to oversight authorities. Yet procurement transparency can be undermined if the system records only final transactions while leaving evaluation logic outside the ledger. A legitimate procurement ledger should therefore connect tender publication, bidder eligibility, evaluation criteria, approval trials, contract variations, and payment milestones. It should also define which information is public, which is available to auditors, and which must remain confidential for lawful commercial reasons. Digital government and public management research jointly suggest that technical reform must be aligned with administrative accountability (Gil-Garcia et al.,2018).

Welfare and social protection payments illustrate the importance of citizen-facing trust. A blockchain-enabled benefit system may reduce duplicate claims, improve traceability of transfers, and support faster reconciliation between treasury systems and service agencies. Nevertheless, such systems also handle highly sensitive data about income, disability, household composition, health status, and vulnerability. A public ledger architecture would be inappropriate for these records. A permissioned architecture with hashed proofs, strict access controls, and clear correction rights is more suitable. The innovation outcome should be evaluated by payment timeliness, reduction in wrongful exclusion, grievance resolution speed, and citizen understanding of benefit status, not only by the number of transactions recorded. The broader connectivity literature underscores that blockchain-enabled public services will increasingly interact with advanced communication infrastructures (Lu and Zheng,2020).

Digital credentials, including educational certificates, professional licenses, business permits, and training records, offer a comparatively low-risk entry point for developing economies. These services benefit from verifiability because employers, universities, regulators, and border agencies often need to confirm credential authenticity. A blockchain credential system can reduce forgery and verification delays while giving citizens portable proof of qualifications. However, the system must preserve the right to update, revoke, or correct credentials. It should also prevent unnecessary disclosure of personal details. Selective disclosure, credential revocation registries, and consent-based verification should be part of the architecture. This domain is especially suitable for early pilots because the service boundary is clear, and the public-value proposition is visible. Public trust studies show that e-government use may affect confidence in government when service experiences are reliable and visible (Tolbert and Mossberger,2006).

Licensing and permitting services can also benefit when administrative steps are distributed across several agencies. Business registration, construction permits, environmental approvals, and transport licenses often require sequential clearance from multiple offices. Blockchain can create a shared status record so that applicants and agencies know which approvals are complete, pending, or disputed. The main goal of government is to avoid automating inefficient procedures without reforming them. If a permit process has unnecessary steps, blockchain may only make delay more traceable rather than reducing it. Public service innovation requires business-process redesign before ledger deployment, including simplification of forms, removal of duplicate approvals, and definition of maximum processing times. Technical overviews of blockchain clarify why consensus, architecture, and data structure choices affect governance implications (Zheng et al.,2017).

Inter-agency data verification is a cross-cutting use case that may generate substantial value without requiring citizens to interact directly with blockchain. Agencies often ask citizens to submit the same documents repeatedly because back-office systems do not trust each other’s records. A permissioned verification ledger can record the fact that a document or status has been validated by an authorized agency, allowing other agencies to rely on that proof. This approach can reduce

administrative burden while limiting the need to share full records. It is particularly useful for identity verification, tax compliance confirmation, company registration status, customs clearance, and eligibility checks. However, legal agreements must define data-sharing authority and liability for incorrect validation. Early e-government research in developing countries highlights both administrative opportunities and the risk of unrealistic implementation assumptions (Ndou,2004).

Public finance monitoring provides another scenario where blockchain can support auditability. Government expenditures, grant disbursements, project milestones, and donor-funded programs often require transparent tracking across agencies and contractors. A ledger can link budget allocation, procurement, contract execution, invoice approval, and payment release. The purpose is not to make every financial detail public, but to create an auditable chain that oversight bodies can examine. Developing economies with limited audit capacity may benefit from automated red-flag rules, but these rules must remain explainable and subject to human review. Smart-contract automation should assist auditors, not replace public accountability judgment. Earlier blockchain reviews also stress that consensus, privacy, scalability, and governance remain open research issues for applied systems (Lu,2018).

Across these scenarios, blockchain's institutional value depends on boundary selection. Large national platforms are politically attractive but difficult to govern. Narrow pilots are easier to manage but may not create systemic value. A balanced approach is to start with a service domain where the record problem is clear, the legal authority is identifiable, stakeholders are limited but relevant, and service outcomes can be measured within a short cycle. Successful pilots can then be expanded through interoperable standards rather than through a single monolithic platform. This modular approach reduces implementation risk and allows governments to learn from service-specific constraints. Collaborative governance theory is relevant because blockchain public services often require joint decision-making across agencies and external partners (Ansell and Gash,2008).

Capacity building should be treated as part of the innovation model. Public agencies need staff who understand not only blockchain terminology, but also data governance, process redesign, procurement risk, privacy protection, and vendor management. Training should be role-specified. Senior officials need to understand strategic value and legal responsibility. IT officers need architecture and cybersecurity knowledge. Legal officers need evidence, liability, and data protection expertise. Frontline officers need workflow procedures and citizen communication skills. Without this layered training, the system may be technically deployed but administratively underused. Systematic blockchain reviews support the need to distinguish architectural promise from empirically demonstrated institutional outcomes (Yli-Huumo et al.,2016).

Citizen communication is equally important. Blockchain language is often abstract, and citizens may not care whether a service uses a ledger. They care whether the service is faster, fairer, safer, and easier to challenge when errors occur. Public communication should therefore avoid exaggerated claims about decentralization and instead explain concrete service changes. Citizens should know what information is recorded, how verification works, why the system is safer than the previous process, and how to seek correction. Trust is strengthened when users can understand the service, not when they are asked to trust technical complexity. Digital strategy research indicates that value emerges when technology is connected to organizational scope, governance, and capabilities (Bharadwaj et al.,2013).

Finally, governments should define performance metrics before deployment. Suitable metrics include average processing time, number of duplicate-document requests, number of detected record inconsistencies, audit completion time, grievance resolution rate, user satisfaction, percentage of transactions with complete metadata, and cost per processed case. These metrics should be compared with a pre-implementation baseline. A blockchain service that cannot demonstrate improvement on such indicators should not be scaled merely because it is technologically advanced. Public service innovation requires measurable value, institutional accountability, and regulatory confidence. Industry 4.0 research reinforces the view that infrastructure innovation requires integration across technical, organizational, and human systems (Lu,2017b).

8. Limitations and Future Research

The first limitation is the use of simulation-calibrated data. The analysis is useful for demonstrating the theoretical model and expected statistical relationships, but it cannot replace field evidence. Future research should collect survey data from public-sector employees, citizens, technology vendors, and regulatory authorities across multiple developing economies. A multi-country design would allow researchers to compare whether institutional trust and regulatory legitimacy function similarly in different administrative traditions. Citizen satisfaction research indicates that public trust is influenced by experienced service

quality, not only by formal transparency claims (Welch et al.,2005).

The second limitation is the focus on perception-based constructions. Perceptions are important because adoption and service use depend on stakeholder beliefs, but public service innovation should also be evaluated through objective indicators. Future studies should measure processing time, dispute frequency, corruption-risk reports, service accessibility, cost changes, data-quality improvements, and citizen satisfaction before and after blockchain implementation. Combining survey data with administrative records would provide a stronger assessment of public value. Blockchain security research also shows why public services must address IoT, data integrity, and cross-system vulnerabilities (Xu et al.,2021).

The third limitation is that the model treats blockchain capability at a general level. Actual technical architecture matters. A permissioned Hyperledger-based registry, an Ethereum-compatible smart-contract system, and a government-controlled hash-anchoring service create different governance implications. Future studies should compare architecture according to validator governance, off-chain storage design, identity management, interoperability standards, and auditability. Technical design should be examined as a source of institutional effects rather than as a background variable. The perceived usefulness and ease-of-use logic remains relevant because frontline officers must still judge whether blockchain systems improve their work (Davis,1989).

The fourth limitation concerns regulatory variation. Developing economies differ in data protection laws, administrative-law traditions, procurement rules, digital identity infrastructure, and judicial capacity. Regulatory legitimacy may therefore have different meanings across contexts. In one country, legitimacy may depend on statutory authorization; in another, it may depend on ministerial guidelines, judicial recognition of digital records, or donor-backed compliance standards. Comparative legal analysis would enrich the model. Advanced machine-learning research signals that public-sector blockchain systems may increasingly intersect with analytics, prediction, and automation (W. Lu et al.,2024).

Future research should also examine unintended consequences. Blockchain can improve auditability, but it can also create permanent records that are difficult to correct, increase surveillance capacity, exclude citizens with weak digital access, or transfer public knowledge to private vendors. These risks are not reasons to reject blockchain outright. They are reasons to build stronger governance safeguards into the design. A mature research agenda should therefore study both innovation benefits and institutional harms. Accountability research clarifies that public agencies must explain who is answerable when a blockchain-enabled process produces harm or error (Bovens,2007).

9. Conclusion

This article developed an institution-centered framework for understanding blockchain-enabled public service innovation in developing economies. Drawing from TOE-based public-sector blockchain adoption research, institutional trust theory, regulatory legitimacy theory, and digital government scholarship, it argued that blockchain capability does not directly produce public service innovation. Instead, blockchain becomes innovative when it strengthens institutional trust, operates under clear regulatory legitimacy, and supports measurable public value. Quantum and industrial information-integration studies illustrate the broader trend toward secure, high-assurance infrastructures for complex systems.

The simulation-calibrated structural analysis illustrated this argument. Blockchain capability was positively associated with institutional trust and regulatory legitimacy, while trust and legitimacy were both associated with public service innovation readiness. The indirect effects through institutional mechanisms were stronger than the direct technology effect, and the interaction between trust and legitimacy showed that each reinforces the other. These results support a practical conclusion: governments should not treat blockchain as a shortcut to trust. They should treat it as a tool that can support trust only when embedded in accountable institutions and lawful service design. Comparative transparency experiments show that trust effects may vary by country and institutional context.

For developing economies, the article recommends a cautious but constructive approach. Blockchain pilots should begin with clear public-service problems, not with technology branding. Legal authority should be mapped before implementation. Sensitive data should be minimized and protected through off-chain storage and role-based access. Oversight should include independent auditability and citizen-facing explanations. Public value should be measured through service outcomes rather than pilot announcements. When these conditions are met, blockchain can support innovation in registries, procurement, welfare delivery, licensing, credential verification, and inter-agency coordination. Future communication infrastructure may

expand the scale and speed of blockchain-enabled services, increasing the importance of governance safeguards.

The broader contribution is to reframe blockchain in government as a legitimacy-sensitive public infrastructure. The central question is not whether distributed ledgers are technically secure, but whether they make public services more trustworthy, lawful, inclusive, and accountable. In developing economies, where administrative capacity and citizen trust are often uneven, this question is decisive. Blockchain-enabled public service innovation will succeed not through code alone, but through the careful alignment of technology, institutions, regulation, and public value. The new public governance perspective supports the article's emphasis on networks, collaboration, and public value creation.

Acknowledgement

The authors gratefully acknowledge the constructive comments of anonymous reviewers and the institutional support provided by their respective universities. No external funding was received for this study. The simulation-calibrated analysis is presented for methodological demonstration and should be validated through future field data collection.

Reference

Tan, E., Mahula, S., & Crompvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for public management. Government Information Quarterly, 39(1), 101625. DOI: https://doi.org/10.1016/j.giq.2021.101625

Lu, Y. (2019b). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80–90. DOI: https://doi.org/10.1016/j.jii.2019.04.002

Carter, L., & Belanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. Information Systems Journal, 15(1), 5–25. DOI: https://doi.org/10.1111/j.1365-2575.2005.00183.x

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. Academy of Management Review, 20(3), 571–610. DOI: https://doi.org/10.5465/amr.1995.9508080331

Batubara, F. R., Ubacht, J., & Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: A systematic literature review. Proceedings of the 19th Annual International Conference on Digital Government Research, 1–9. DOI: https://doi.org/10.1145/3209281.3209317

Avgerou, C. (2008). Information systems in developing countries: A critical research review. Journal of Information Technology, 23(3), 133–146. DOI: https://doi.org/10.1057/palgrave.jit.2000136

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1–2), 2448003. DOI: https://doi.org/10.1080/17517575.2024.2448003

Belanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. Journal of Strategic Information Systems, 17(2), 165–176. DOI: https://doi.org/10.1016/j.jsis.2007.12.002

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. American Journal of Sociology, 83(2), 340–363. DOI: https://doi.org/10.1086/226550

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. DOI: https://doi.org/10.1016/j.giq.2017.09.007

Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). Digital innovation management: Reinventing innovation management research in a digital world. MIS Quarterly, 41(1), 223–238. DOI: https://doi.org/10.25300/MISQ/2017/41:1.03

Heeks, R. (2002). Information systems and developing countries: Failure, success, and local improvisations. The Information Society, 18(2), 101–112. DOI: https://doi.org/10.1080/01972240290075039

Bustamante, P., Micheli, M., Geva, B., & Livermore, M. A. (2022). Government by code? Blockchain applications to public sector governance. Frontiers in Blockchain, 5, 869665. DOI: https://doi.org/10.3389/fbloc.2022.869665

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876–1907. DOI: https://doi.org/10.1080/17517575.2021.2008513

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478. DOI: https://doi.org/10.2307/30036540

Grimmelikhuijsen, S. G., & Meijer, A. J. (2014). Effects of transparency on the perceived trustworthiness of a government organization: Evidence from an online experiment. Journal of Public Administration Research and Theory, 24(1), 137–157. DOI: https://doi.org/10.1093/jopart/mus048

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. DOI: https://doi.org/10.1016/j.tele.2018.11.006

Shareef, M. A., Kumar, V., Kumar, U., & Dwivedi, Y. K. (2011). E-government Adoption Model (GAM): Differing service maturity levels. Government Information Quarterly, 28(1), 17–35. DOI: https://doi.org/10.1016/j.giq.2010.05.006

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160. DOI: https://doi.org/10.2307/2095101

Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9), 2397630. DOI: https://doi.org/10.1080/17517575.2024.2397630

Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Fernandez-Gutierrez, M. (2023). Blockchain in government: Toward an evaluation framework. Policy Design and Practice, 6(4), 398–418. DOI: https://doi.org/10.1080/25741292.2023.2230702

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). The new organizing logic of digital innovation: An agenda for information systems research. Information Systems Research, 21(4), 724–735. DOI: https://doi.org/10.1287/isre.1100.0322

Walsham, G., & Sahay, S. (2006). Research on information systems in developing countries: Current landscape and future prospects. Information Technology for Development, 12(1), 7–24. DOI: https://doi.org/10.1002/itdj.20020

Smits, M., & Hulstijn, J. (2020). Blockchain applications and institutional trust. Frontiers in Blockchain, 3, 5. DOI: https://doi.org/10.3389/fbloc.2020.00005

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118–144. DOI: https://doi.org/10.1016/j.jsis.2019.01.003

Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), 1939895. DOI: https://doi.org/10.1080/17517575.2021.1939895

Cordella, A., & Bonina, C. M. (2012). A public value perspective for ICT enabled public sector reforms: A theoretical reflection. Government Information Quarterly, 29(4), 512–520. DOI: https://doi.org/10.1016/j.giq.2012.03.004

Oliver, C. (1991). Strategic responses to institutional processes. Academy of Management Review, 16(1), 145–179. DOI: https://doi.org/10.5465/amr.1991.4279002

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038. DOI: https://doi.org/10.1016/j.telpol.2017.09.003

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. Government Information Quarterly, 32(3), 221–236. DOI: https://doi.org/10.1016/j.giq.2015.07.001

Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103–2115. DOI: https://doi.org/10.1109/JIOT.2018.2869847

Levi, M., & Stoker, L. (2000). Political trust and trustworthiness. Annual Review of Political Science, 3, 475–507. DOI: https://doi.org/10.1146/annurev.polisci.3.1.475

Beck, R., Muller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. Journal of the Association for Information Systems, 19(10), 1020–1034. DOI: https://doi.org/10.17705/1jais.00518

Twizeyimana, J. D., & Andersson, A. (2019). The public value of e-government: A literature review. Government Information Quarterly, 36(2), 167–178. DOI: https://doi.org/10.1016/j.giq.2019.01.001

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. DOI: https://doi.org/10.1016/j.jii.2021.100224

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model. International Journal of Electronic Commerce, 7(3), 101–134. DOI: https://doi.org/10.1080/10864415.2003.11044275

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135. DOI: https://doi.org/10.1080/00207543.2018.1533261

Janssen, M., & van der Voort, H. (2016). Adaptive governance: Towards a stable, accountable and responsive government. Government Information Quarterly, 33(1), 1–5. DOI: https://doi.org/10.1016/j.giq.2016.02.003

Zucker, L. G. (1987). Institutional theories of organization. Annual Review of Sociology, 13, 443–464. DOI: https://doi.org/10.1146/annurev.so.13.080187.002303

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715–1729. DOI: https://doi.org/10.1007/s10796-022-10248-7

Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Management: An International Journal, 23(6), 545–559. DOI: https://doi.org/10.1108/SCM-01-2018-0029

Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government: A framework and programme for research. Government Information Quarterly, 31(1), 119–128. DOI: https://doi.org/10.1016/j.giq.2013.06.002

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334–359. DOI: https://doi.org/10.1287/isre.13.3.334.81

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80–89. DOI: https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Hartley, J. (2005). Innovation in governance and public services: Past and present. Public Money & Management, 25(1), 27–34. DOI: https://doi.org/10.1111/j.1467-9302.2005.00447.x

Lu, Y., & Yang, J. (2024). Quantum financing system: A survey on quantum algorithms, potential scenarios and open research issues. Journal of Industrial Information Integration, 41, 100663. DOI: https://doi.org/10.1016/j.jii.2024.100663

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. Government Information Quarterly, 36(4), 101385. DOI: https://doi.org/10.1016/j.giq.2019.06.002

Rothstein, B., & Stolle, D. (2008). The state and social capital: An institutional theory of generalized trust. Comparative Politics, 40(4), 441–459. DOI: https://doi.org/10.5129/001041508X12911362383354

Risius, M., & Spohrer, K. (2017). A blockchain research framework: What we do not know, where we go from here, and how we will get there. Business & Information Systems Engineering, 59(6), 385–409. DOI: https://doi.org/10.1007/s12599-017-0506-0

Schuppan, T. (2009). E-government in developing countries: Experiences from sub-Saharan Africa. Government Information Quarterly, 26(1), 118–127. DOI: https://doi.org/10.1016/j.giq.2008.01.006

Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 34. DOI: https://doi.org/10.1186/s40854-024-00668-6

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. Journal of Management Information Systems, 19(4), 9–30. DOI: https://doi.org/10.1080/07421222.2003.11045748

Hyvarinen, H., Risius, M., & Friis, G. (2017). A blockchain-based approach towards overcoming financial fraud in public sector services. Business & Information Systems Engineering, 59(6), 441–456. DOI: https://doi.org/10.1007/s12599-017-0502-4

Gil-Garcia, J. R., Dawes, S. S., & Pardo, T. A. (2018). Digital government and public management research: Finding the crossroads. Public Management Review, 20(5), 633–646. DOI: https://doi.org/10.1080/14719037.2017.1327181

Lu, Y., & Zheng, X. (2020). 6G: A survey on technologies, scenarios, challenges, and the related issues. Journal of Industrial Information Integration, 19, 100158. DOI: https://doi.org/10.1016/j.jii.2020.100158

Tolbert, C. J., & Mossberger, K. (2006). The effects of e-government on trust and confidence in government. Public Administration Review, 66(3), 354–369. DOI: https://doi.org/10.1111/j.1540-6210.2006.00594.x

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

Ndou, V. (2004). E-government for developing countries: Opportunities and challenges. Electronic Journal of Information Systems in Developing Countries, 18(1), 1–24. DOI: https://doi.org/10.1002/j.1681-4835.2004.tb00117.x

Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 5(4), 231–255. DOI: https://doi.org/10.1080/23270012.2018.1516523

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. Journal of Public Administration Research and Theory, 18(4), 543–571. DOI: https://doi.org/10.1093/jopart/mum032

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. PLOS ONE, 11(10), e0163477. DOI: https://doi.org/10.1371/journal.pone.0163477

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. MIS Quarterly, 37(2), 471–482. DOI: https://doi.org/10.25300/MISQ/2013/37.2.3

Lu, Y. (2017b). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1–10. DOI: https://doi.org/10.1016/j.jii.2017.04.005

Welch, E. W., Hinnant, C. C., & Moon, M. J. (2005). Linking citizen satisfaction with e-government and trust in government. Public Administration Review, 65(3), 371–382. DOI: https://doi.org/10.1111/j.1540-6210.2005.00442.x

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452–10473. DOI: https://doi.org/10.1109/JIOT.2021.3060508

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. DOI: https://doi.org/10.2307/249008

Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., & Ivanov, L. A. (2024). Quantum machine learning: Classifications, challenges, and solutions. Journal of Industrial Information Integration, 42, 100736. DOI: https://doi.org/10.1016/j.jii.2024.100736

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. European Law Journal, 13(4), 447–468. DOI: https://doi.org/10.1111/j.1468-0386.2007.00378.x

Lu, Y., Sigov, A. S., Ratkin, L., Ivanov, L. A., & Zuo, M. (2023). Quantum computing and industrial information integration: A review. Journal of Industrial Information Integration, 35, 100511. DOI: https://doi.org/10.1016/j.jii.2023.100511

Grimmelikhuijsen, S., Porumbescu, G., Hong, B., & Im, T. (2013). The effect of transparency on trust in government: A cross-national comparative experiment. Public Administration Review, 73(4), 575–586. DOI: https://doi.org/10.1111/puar.12047

Lu, Y., & Ning, X. (2020). A vision of 6G–5G's successor. Journal of Management Analytics, 7(3), 301–320. DOI: https://doi.org/10.1080/23270012.2020.1802622

Osborne, S. P. (2006). The new public governance? Public Management Review, 8(3), 377–387. DOI: https://doi.org/10.1080/14719030600853022

Ye, Z., & Lu, Y. (2022). Quantum science: A review and current research trends. Journal of Management Analytics, 9(3), 383–402. DOI: https://doi.org/10.1080/23270012.2022.2089064

Yoo, Y., Boland, R. J., Lyytinen, K., & Majchrzak, A. (2012). Organizing for innovation in the digitized world. Organization Science, 23(5), 1398–1408. DOI: https://doi.org/10.1287/orsc.1120.0771

Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215–234. DOI: https://doi.org/10.1007/s10796-021-10221-w

Porumbescu, G. A. (2016). Linking public sector social media and e-government website use to trust in government. Government Information Quarterly, 33(2), 291–304. DOI: https://doi.org/10.1016/j.giq.2016.04.006

Dimitropoulos, G. (2022). The use of blockchain by international organizations: Effectiveness and legitimacy. Policy and Society, 41(3), 328–342. DOI: https://doi.org/10.1093/polsoc/puab021

Fichman, R. G., Dos Santos, B. L., & Zheng, Z. E. (2014). Digital innovation as a fundamental and powerful concept in the information systems curriculum. MIS Quarterly, 38(2), 329–353. DOI: https://doi.org/10.25300/MISQ/2014/38.2.01

Hinings, B., Gegenhuber, T., & Greenwood, R. (2018). Digital innovation and transformation: An institutional perspective. Information and Organization, 28(1), 52–61. DOI: https://doi.org/10.1016/j.infoandorg.2018.02.004

Srivastava, S. C., & Teo, T. S. H. (2007). E-government payoffs: Evidence from cross-country data. Journal of Global Information Management, 15(4), 20–40. DOI: https://doi.org/10.4018/jgim.2007100102