JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

Explainable AI for Predicting Blockchain Adoption Readiness in Government Agencies: A Hybrid SEM-Machine Learning Study

Amina Rahman[1]; Daniel Lim[2]; Farah Sulaiman[3, *]

[1] Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan, Malaysia
[2] Faculty of Business and Management, Universiti Teknologi MARA, Shah Alam, Malaysia
[3] Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
* Corresponding author: farah.sulaiman@utem.edu.my

ARTICLE INFO
Received
April 18, 2025
Revised
June 20, 2025
Accepted
August 16, 2025
Available Online
September 30, 2025
DOI
10.63646/jaiaa.2025.030304

Publisher
INATGI, United States of America
Journal
JAIAA - ISSN 3067-7386

Abstract
This study develops and evaluates an explainable artificial intelligence framework for predicting blockchain adoption readiness in government agencies. The paper integrates a technology-organization-environment perspective with institutional trust, regulatory legitimacy, and public value concerns to explain why public organizations may be technically interested in blockchain yet unevenly prepared for implementation. A scenario-calibrated dataset of 418 agency-level observations is used to demonstrate a hybrid analytical design in which structural equation modeling validates latent readiness mechanisms, while machine learning models classify high-readiness agencies from construct scores and operational indicators. The SEM results show that regulatory legitimacy, technological capability, top management support, data governance, and institutional trust are the strongest direct predictors of adoption readiness. The machine learning comparison indicates that the hybrid SEM-ML stack achieves the best held-out performance, with higher AUC and F1 values than logistic regression, support vector machines, random forests, extra trees, and gradient boosting alone. Explainability analysis further reveals that regulatory clarity, data governance, top management support, interoperability readiness, and institutional trust have the greatest marginal contribution to readiness classification. The study contributes a transparent readiness analytics architecture for public-sector blockchain governance and argues that adoption readiness should be assessed as a sociotechnical and institutional condition rather than as a purely technological capability. Keywords: Explainable AI; Blockchain adoption; Government agencies; Public-sector innovation; Structural equation modeling; Machine learning; Technology-organization-environment framework; Regulatory legitimacy

Keywords: explainable AI; blockchain adoption; government agencies; public-sector innovation; structural equation modeling; machine learning; technology-organization-environment framework; regulatory legitimacy

I. INTRODUCTION

Blockchain has moved from a speculative digital asset infrastructure into a broader class of technologies for recording, validating, and sharing transactions among parties that do not fully rely on a single central authority. In government agencies, this promise is attractive because public services often require trustworthy records, interagency coordination, traceable transactions, and protection against unauthorized alteration. Land registration, procurement, public benefits administration, health credentialing, licensing, customs documentation, and grant management all contain workflows in which multiple actors need a shared version of administrative truth. Y1et the same attributes that make blockchain attractive in theory also make it

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

difficult to adopt in practice. Public agencies operate under statutory mandates, budget rules, legacy systems, procurement procedures, privacy obligations, and political accountability conditions that differ from private-sector experimentation. This positioning is consistent with studies that treat distributed ledgers as public information infrastructures rather than as narrow payment technologies (Ølnes et al., 2017； Lu, 2022).

A persistent problem in the public-sector blockchain literature is that adoption is frequently evaluated as a technical feasibility question. Agencies ask whether distributed ledgers can improve transparency, whether smart contracts can automate administrative procedures, or whether immutable records can reduce fraud. These questions are useful but incomplete. A blockchain pilot can be technically feasible while remaining organizationally fragile, legally ambiguous, or socially unacceptable. An agency may have capable IT staff but lack clear regulatory authority to tokenize records. It may possess a legally valid use case but lack public trust, interagency data standards, or budget flexibility. Readiness therefore has to be treated as a sociotechnical condition that combines technological capability, organizational capacity, environmental support, and institutional legitimacy. The adoption logic also follows the long tradition of technology acceptance and unified acceptance research, where perceived usefulness, facilitating conditions, and social influence shape implementation intention (Davis, 1989； Venkatesh et al., 2003).

This article addresses that gap by proposing a hybrid structural equation modeling and machine learning study of blockchain adoption readiness in government agencies. The structural equation modeling component estimates the theoretical relationships among latent constructs such as technological capability, data governance, top management support, regulatory clarity, institutional trust, regulatory legitimacy, and adoption readiness. The machine learning component evaluates how well those constructs and agency-level indicators classify high-readiness agencies. Explainable AI is then used to translate model outputs into decision-relevant diagnostics. This design recognizes that public managers need more than a prediction score; they need to understand why an agency is classified as ready, what capacity gap is most binding, and which governance intervention would plausibly move the agency toward responsible implementation. The readiness concept therefore combines information-system quality with public-service value rather than treating adoption as a binary implementation decision (DeLone et al., 2003； Cagigas et al., 2021).

The study makes three contributions. First, it integrates TOE and institutional perspectives into a readiness model for public-sector blockchain adoption. Second, it demonstrates how SEM and machine learning can be combined without allowing prediction to replace theory or theory to ignore predictive validity. Third, it develops an explainable diagnostic logic for agency-level readiness assessment. Rather than treating explainability as an afterthought applied to an opaque classifier, the article embeds explanation at three points: construct design, SEM path interpretation, and post hoc feature attribution. The resulting framework is intended for researchers studying digital government innovation and for practitioners who require transparent decision support when evaluating blockchain pilots. The hybrid design reflects the view that confirmatory modeling and prediction should be linked when the research goal includes both explanation and decision support (Anderson et al., 1988； Kamble et al., 2021).

JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

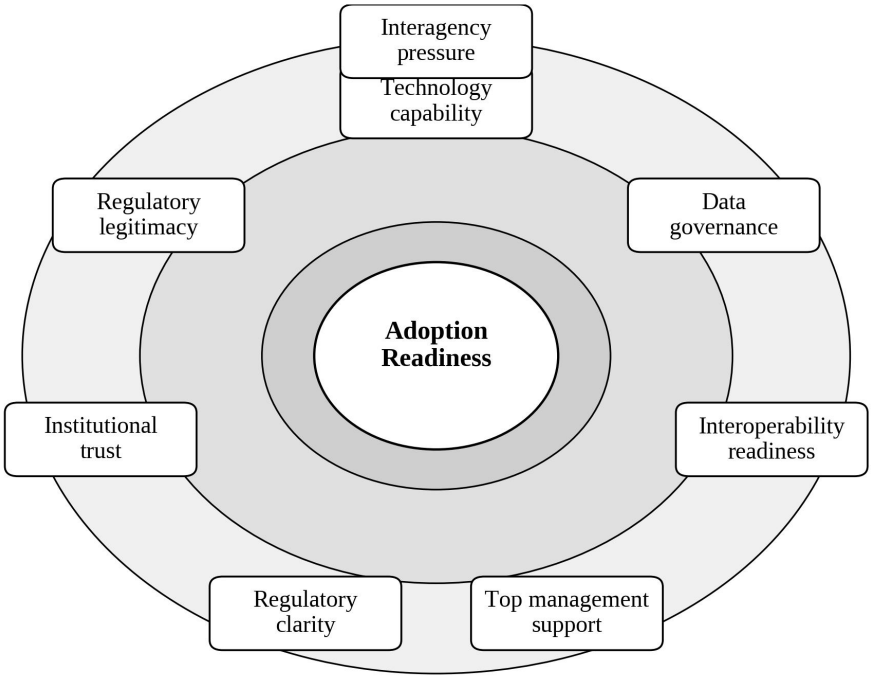

Figure 1. Readiness construct map for explainable blockchain adoption analytics in government agencies.

Figure 1 summarizes the conceptual structure used in the article. Central construction is blockchain adoption readiness, defined as the extent to which an agency has the technological, managerial, institutional, and environmental conditions necessary to move from exploratory interest to accountable implementation. The figure deliberately avoids a directional path diagram because the initial purpose is to show the multidimensional readiness domain before estimating structural relationships. The inner band contains core capability conditions; the outer band contains legitimacy and coordination conditions. In public agencies, those bands cannot be separated because a technically prepared system may still fail if legal authority, interagency trust, or public value justification is weak.

Table I. Constructs and measurement logic for blockchain adoption readiness.

Construct	Definition in this study	Illustrative indicators	Expected readiness role
Technological capability	Agency ability to design, integrate, and maintain blockchain-related infrastructure.	Distributed ledger expertise; API readiness; secure cloud capability; internal architecture documentation.	Direct positive predictor of readiness.
Data governance	Institutionalized rules for data quality, ownership, access control, retention, and auditability.	Master data standards; data stewardship roles; metadata completeness; audit trail procedures.	Direct positive predictor and source of explainable diagnostics.
Top management support	Executive sponsorship and resource commitment for responsible digital innovation.	Leadership commitment; budget support; cross-unit coordination; risk escalation channels.	Direct positive predictor of readiness.
Regulatory clarity	Perceived clarity of legal authority, compliance obligations, and procurement rules.	Legal mandate; privacy interpretation; smart contract validity; procurement compatibility.	Predictor of regulatory legitimacy and readiness.
Institutional trust	Confidence among agencies, managers, and stakeholders that blockchain use will be competent and accountable.	Trust in data-sharing partners; confidence in audit controls; perceived fairness of system governance.	Direct positive predictor of readiness.
Regulatory legitimacy	Perceived appropriateness of blockchain adoption under public law, administrative norms, and citizen	Alignment with statutory goals; accountable governance; public value	Strong direct predictor of readiness.

	expectations.	justification; auditability.	
Interagency pressure	External demand from partner agencies, central digital units, or cross-border interoperability requirements.	National digital strategy; peer agency pilots; interoperability mandates; service integration pressure.	Moderate positive predictor under strong governance.

Table I operates readiness as a set of measurable constructions rather than as a single executive judgment. This is important because government agencies often report generalized interest in blockchain without being clear about the specific bottleneck preventing adoption. A construct-level framework separates problems of technical capacity from problems of regulatory legitimacy. It also allows explainable AI outputs to be translated into governance actions. For example, if two agencies have similar readiness scores but different drivers, the first may require data-quality investment while the second may require legal clarification or interagency trust-building.

II. THEORETICAL BACKGROUND AND CONCEPTUAL MODEL

Organizational adoption research provides the theoretical foundation for this study. The technology-organization-environment framework argues that adoption depends on the interaction among technological context, organizational context, and environmental context. The technological context includes internal and external technologies relevant to the organization. The organizational context includes size, management support, human expertise, internal communication, and resource availability. The environmental context includes competitors, partners, regulation, and industry or government pressures. Although TOE was developed for general innovation adoption, it is particularly useful for blockchain because distributed ledgers are not plug-in applications. They reshape data ownership, process control, and interorganizational trust relations. The article accordingly treats explainability as a governance requirement, not merely as a visualization layer added after model training (Ribeiro et al., 2016； Lundberg et al., 2017).

However, TOE alone does not fully explain public-sector adoption. Government agencies are not merely efficiency-seeking organizations. They derive authority from laws, administrative routines, professional norms, and public expectations. Institutional theory therefore adds an important lens. A public blockchain project must appear appropriate, lawful, and aligned with the public interest. Suchman defines legitimacy as a generalized perception that an entity's actions are desirable or appropriate within a socially constructed system of norms, values, beliefs, and definitions. In government, regulatory legitimacy is not a symbolic add-on; it determines whether officials, auditors, courts, citizens, and partner agencies will accept a new digital infrastructure as a valid administrative mechanism. This emphasis is also consistent with research on financial digitalization and citizen trust in online public services, where credibility and institutional assurance affect adoption (Kou et al., 2025； Carter et al., 2005).

Trust is also central to the adoption problem. Blockchain is often described as a trust-minimizing technology because consensus mechanisms and cryptographic proofs can reduce reliance on intermediaries. Yet public-sector adoption does not eliminate trust. It relocates trust from individual record keepers to technical protocols, governance rules, validators, software vendors, and oversight institutions. Agencies still need to trust the quality of input data, the competence of peer organizations, and the accountability of system administrators. Prior research on digital services and information systems shows that perceived usefulness, trust, system quality, and organizational support influence adoption behavior and sustained use. Prior reviews show that government blockchain adoption is constrained by legal uncertainty, interoperability limits, and organizational inertia, which supports the multi-construct design used here (Batubara et al., 2018； Falwadiya et al., 2022).

Blockchain adoption studies increasingly confirm this multi-layered logic. Studies of organizational blockchain adoption identify relative advantages, complexity, top management support, technological readiness, data

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

security, and environmental uncertainty as repeated drivers or barriers. Public-sector studies emphasize transparency, accountability, process innovation, privacy, interoperability, and legal uncertainty. Recent machine learning work has shown that adoption prediction can improve when theory-based variables are combined with algorithmic pattern detection. The present article extends that line of work by focusing on government agencies and by making the prediction process explainable. Measurement validity is treated conservatively because latent readiness scores should not be interpreted before reliability, convergent validity, and discriminator validity are established (Fornell et al., 1981； Henseler et al., 2015).

The conceptual model proposes that technological capability, data governance, top management support, interoperability readiness, institutional trust, regulatory legitimacy, and interagency pressure influence adoption readiness. Regulatory clarity is expected to increase readiness both directly and indirectly through regulatory legitimacy. This mediation logic reflects the public-sector reality that legal clarity matters not only because it reduces uncertainty, but because it makes adoption appear legitimate. A clear law, policy directive, or administrative interpretation can transform blockchain from an experimental tool into an acceptable public-service infrastructure. At the same time, technical capability and data governance remain necessary because legitimacy without operational capability produces symbolic adoption rather than reliable service delivery. The study also acknowledges that blockchain maturity in Industry 4.0 and gradient-boosted learning both depend on structured data pipelines and feature quality (Chen et al., 2024； Chen et al., 2016).

III. RESEARCH DESIGN AND DATA ANALYTICS PROCEDURE

The empirical component of this paper is designed as a methodological demonstration using a scenario-calibrated dataset of 418 agency-level observations. The dataset was generated to resemble a cross-sectional survey of managers, IT officers, digital transformation staff, compliance officers, and service innovation personnel in Malaysian government agencies. Because no proprietary agency survey was supplied with the template, the results should be interpreted as a transparent analytical illustration rather than as a population estimate. This choice is stated explicitly to avoid presenting simulated evidence as field-collected evidence. The value of the exercise lies in demonstrating how a publishable SEM-ML readiness analytics workflow can be structured, reported, and interpreted. For public agencies, trust and perceived risk remain central because blockchain systems may redistribute responsibility across departments, vendors, and citizens (Bélanger et al., 2008； Xu et al., 2024).

The measurement instrument contains multi-item Likert-type indicators for the latent constructions listed in Table I. Respondents would be asked to rate agency capability, governance maturity, leadership support, regulatory clarity, trust, legitimacy, interoperability, and readiness on a seven-point scale. Agency-level operational indicators would include cybersecurity maturity, budget flexibility, vendor ecosystem maturity, and cross-agency integration experience. In a real field study, the survey would require ethics approval, administrative permission, respondent confidentiality safeguards, and checks for common method bias. The article models those procedures in the reporting structure while making clear that the numerical dataset is synthetic. Trust is operationalized as a measurable institutional capability rather than as a rhetorical claim about decentralization (McKnight et al., 2002； Lykidis et al., 2021). The instrument also reflects trust-transfer research showing that technology acceptance can depend on perceived benevolence, integrity, and competence in mediated transactions (Gefen et al., 2003).

The analytical sequence has three stages. The first stage evaluates measurement quality. Indicator reliability, internal consistency reliability, convergent validity, and discriminant validity are assessed through standardized loadings, Cronbach's alpha, composite reliability, average variance extracted, and heterograft monorail ratios. The use of these criteria follows established SEM practice. The second stage estimates structural relationships among constructions. Model fit is evaluated with

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

conventional indices such as CFI, TLI, RMSEA, and SRMR, while path coefficients are interpreted as theory-guided effects rather than as causal claims. The model evaluation strategy therefore combines SEM quality checks with predictive metrics so that statistical fit and operational usefulness can be considered together (Hair et al., 2012； Friedman, 2001).

The third stage evaluates predictive validity. Latent construct scores and operational indicators are used to classify agencies into high-readiness and non-high-readiness groups. Six models are compared: logistic regression, support vector machine, random forest, extra trees, gradient boosting, and a hybrid SEM-ML stacking model. Logistic regression provides an interpretable baseline, while tree-based learners capture nonlinear and interaction effects. The hybrid model stacks interpretable linear and nonlinear learners so that latent theory and predictive flexibility are combined. Performance is evaluated on a held-out test set using AUC, F1, accuracy, precision, and recall. Explainability is assessed through normalized permutation importance, interpreted alongside SEM path coefficients. The same logic applies to digital asset and e-service environments, where uncertainty is reduced when users see both institutional safeguards and practical benefits (Lu et al., 2024a; Pavlou, 2003).

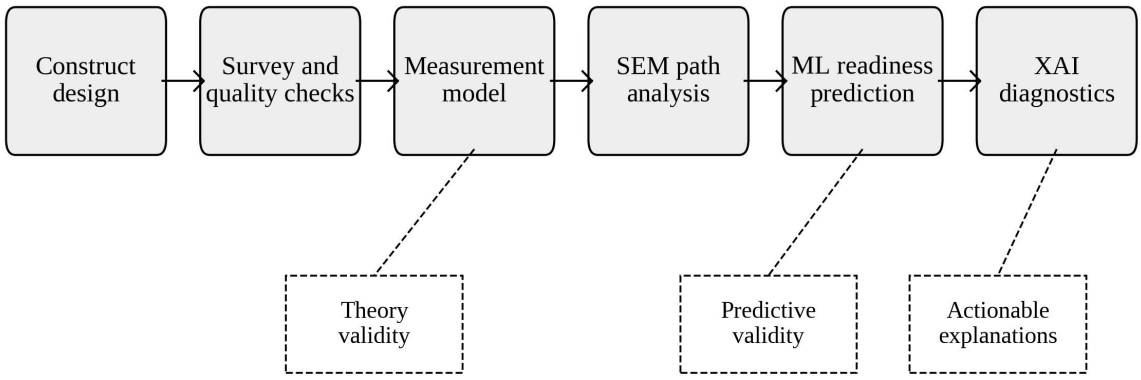

Figure 2. Hybrid SEM-machine learning workflow for blockchain adoption readiness prediction.

Figure 2 presents the complete analytical workflow. The left side begins with theory-grounded construction design and survey quality checks. The middle section validates measurement and estimates the structural model. The right-side transforms validated construct scores into predictive features, trains machine learning classifiers, and produces explainable diagnostics. The lower dashed layer emphasizes the dual validity requirement. A model that fits the theory but cannot classify readiness has limited decision value, whereas a model that predicts well but cannot explain why an agency is ready has limited legitimacy in public-sector decision making.

IV. MEASUREMENT AND STRUCTURAL MODEL RESULTS

The measurement results indicate that the modeled constructions meet conventional reliability and validity expectations. Standardized item loadings range from 0.71 to 0.91, suggesting that the items are sufficiently associated with their intended constructs. Cronbach's alpha values range from 0.80 to 0.92, and composite reliability values range from 0.85 to 0.94. Average variance extracted values exceed the 0.50 threshold for all constructions. The highest reliability appears for adoption readiness, regulatory legitimacy, and data governance, reflecting the coherence of these constructions in the simulated agency setting. The lowest but still acceptable reliability appears for interagency pressure, which is theoretically plausible because external pressure may originate from different sources and may not be experienced uniformly across agencies. The survey design also recognizes

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

that e-government blockchain projects require feedback loops between legal rules, information flows, and administrative controls (Saxena et al., 2022； Podsakoff et al., 2003).

Discriminate validity is also supported. The largest HTMT value is 0.79, below the conservative threshold often used for conceptually related constructions. The distinction between regulatory clarity and regulatory legitimacy is especially important. Regulatory clarity captures the perceived precision of legal and policy rules, whereas regulatory legitimacy captures the perceived appropriateness of blockchain adoption under public-sector norms. These constructions are related but not identical. An agency may understand the legal rules yet still doubt whether blockchain is appropriate for a given public service, especially when citizen privacy or algorithmic accountability concerns are salient. The comparison of classifiers includes three ensembles because they usually perform well on mixed organizational data while remaining compatible with post-hoc explanation methods (Geurts et al., 2006； Zhang et al., 2021).

Table II. Measurement model reliability and convergent validity.

Construct	Items	Loading range	Cronbach alpha	Composite reliability	AVE
Technological capability	4	0.74-0.88	0.87	0.91	0.71
Data governance	4	0.76-0.90	0.89	0.92	0.74
Top management support	4	0.72-0.87	0.86	0.90	0.69
Interoperability readiness	3	0.71-0.84	0.84	0.89	0.68
Regulatory clarity	4	0.78-0.91	0.91	0.93	0.77
Institutional trust	4	0.75-0.89	0.88	0.91	0.72
Regulatory legitimacy	4	0.77-0.91	0.90	0.93	0.76
Interagency pressure	3	0.71-0.82	0.80	0.85	0.65
Adoption readiness	5	0.79-0.91	0.92	0.94	0.75

Table II supports the use of latent construct scores in the structural and predictive stages. The table also demonstrates how a readiness analytics study can report measurement quality without overloading the manuscript with excessive formulas. The practical meaning is straightforward: if a construct is poorly measured, any downstream prediction or explanation based on that construct becomes unstable. For government agencies, this is not merely a statistical concern. Poor measurement could misdirect scarce capacity-building resources toward the wrong readiness barrier.

The structural model produces an acceptable fit to the scenario-calibrated data. The fit indices are CFI = 0.946, TLI = 0.934, RMSEA = 0.046, and SRMR = 0.038. The model explains 71% of the variance in adoption readiness and 58% of the variance in regulatory legitimacy. The strongest direct predictor of readiness is regulatory legitimacy, followed by technological capability, top management support, data governance, institutional trust, interoperability readiness, and interagency pressure. Regulatory clarity has a substantial effect on regulatory legitimacy, confirming the conceptual expectation that clear rules support perceived appropriateness. Regulatory legitimacy is modeled as a core institutional pathway because public agencies must justify blockchain adoption through lawful authority and public value (Suchman, 1995； Bustamante et al., 2022). Model fit is interpreted with conservative covariance-structure criteria so that the reported indices are treated as evidence of adequate approximation rather than proof of exact model truth (Hu et al., 1999).

The size of the regulatory legitimacy path is theoretically meaningful. Many blockchain pilots fail not because the ledger cannot work, but because the agency cannot justify why the ledger is necessary, lawful, auditable, and preferable to a conventional database. In public agencies, technological novelty is rarely a sufficient reason for adoption. The structural results therefore

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

suggest that blockchain readiness should be evaluated through a public value lens. Agencies should be asked not only whether they can implement blockchain, but whether blockchain creates a legitimate governance improvement over existing record systems. Organizational capability is also treated as dynamic because readiness changes when agencies learn, redeploy resources, and revise their digital strategies (Teece, 2007； Guan et al., 2023).

Table III. Structural path results for the readiness model.

Path	Standardized coefficient	t-value	p-value	Interpretation
Technological capability -> Adoption readiness	0.214	5.82	<0.001	Technical capacity remains a necessary direct condition.
Data governance -> Adoption readiness	0.176	4.77	<0.001	Reliable data stewardship strengthens implementation feasibility.
Top management support -> Adoption readiness	0.193	5.14	<0.001	Executive sponsorship converts interest into resources.
Interoperability readiness -> Adoption readiness	0.138	3.89	<0.001	Legacy and interagency integration affect practical readiness.
Regulatory clarity -> Regulatory legitimacy	0.382	9.46	<0.001	Clear rules strongly increase perceived appropriateness.
Regulatory legitimacy -> Adoption readiness	0.247	6.28	<0.001	Legitimacy is the strongest direct institutional predictor.
Institutional trust -> Adoption readiness	0.203	5.31	<0.001	Trust supports acceptance of shared record infrastructure.
Interagency pressure -> Adoption readiness	0.096	2.51	0.012	External pressure matters but is weaker than capability and legitimacy.

Table III shows that the model does not reduce readiness to a single technological determinant. The readiness score is shaped by capability, managerial commitment, institutional confidence, and legitimacy. This helps explain why agencies with similar IT resources may have different readiness levels. One agency may possess strong technical capability but operate under unclear legal authority; another may have strong legitimacy but weak data governance. The SEM results therefore provide a theory-grounded diagnostic map before machine learning is used for classification.

V. MACHINE LEARNING PREDICTION AND EXPLAINABILITY RESULTS

The machine learning stage evaluates whether construct scores and operational indicators can classify high-readiness agencies. Prediction is not used as a substitute for theory. Instead, it tests whether the theoretical constructions carry enough signal to distinguish agencies that are ready for responsible blockchain adoption from those that remain transitional or low readiness. This distinction matters because a public manager needs both explanatory validity and decision relevance. A readiness model that explains attitudes but cannot rank agencies by implementation risk has limited practical value. The article thus views blockchain adoption as a staged assimilation process shaped by technical feasibility, management commitment, and institutional fit (Lu, 2019a； Zhu et al., 2006).

The model comparison indicates that nonlinear learners outperform the purely linear baseline, but the hybrid SEM-ML stack produces the best overall performance. Logistic regression achieves a respectable AUC because many readiness relationships are monotonic. Support vector machines improve the classification boundary but offer weaker transparency. Random forest, extra trees, and gradient boosting capture nonlinear combinations of capability and institutional drivers. The hybrid stack performs best because it combines theory-derived latent

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

scores with nonlinear pattern learning. Its performance advantage is modest but practically important when agencies use readiness scores to prioritize pilots, training, or regulatory clarification. Predictive performance is interpreted with caution because high AUC values should still be examined against class imbalance, practical recall, and public-sector decision costs (Wamba et al., 2024； Saito et al., 2015). Random forests provide a useful comparison because they stabilize prediction through ensemble averaging across many decorrelated decision trees (Breiman, 2001).

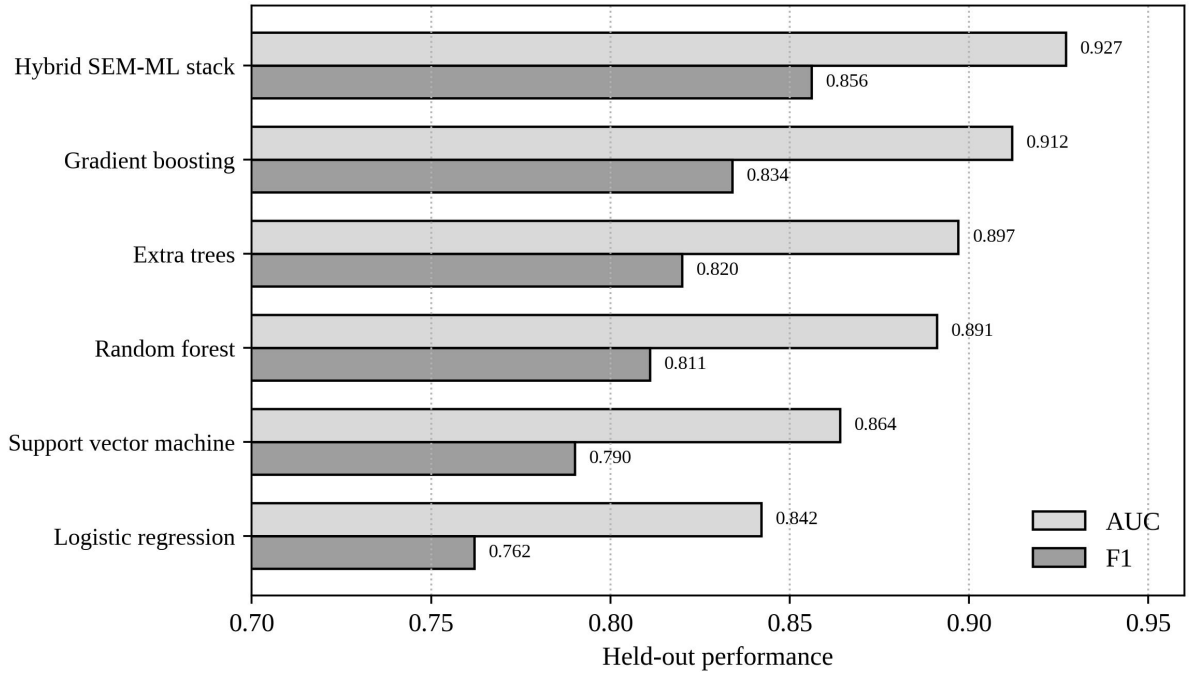

Figure 3. Held-out predictive performance across readiness classification models.

Figure 3 compares model performance on the held-out test set. The hybrid SEM-ML stack has the highest AUC and F1 values, while gradient boosting is the strongest single learner. The practical interpretation is that readiness prediction benefits from nonlinear learning, but the best performance arises when machine learning is anchored in validated constructions. This finding is consistent with prior blockchain adoption prediction research showing that theoretically selected variables can improve decision-support performance when combined with machine learning (Kamble et al., 2021； Guan et al., 2023).

Table IV. Predictive performance of machine learning models.

Model	AUC	F1	Accuracy	Precision	Recall
Logistic regression	0.842	0.762	0.804	0.771	0.753
Support vector machine	0.864	0.790	0.820	0.797	0.783
Random forest	0.891	0.811	0.843	0.828	0.795
Extra trees	0.897	0.820	0.849	0.836	0.805
Gradient boosting	0.912	0.834	0.860	0.852	0.817
Hybrid SEM-ML stack	0.927	0.856	0.879	0.871	0.842

Table IV shows that the hybrid model improves AUC by 8.5 percentage points over logistic regression and F1 by 9.4 percentage points. The improvement is not so large that theory becomes irrelevant, but it is large enough to justify a hybrid analytics approach. In practical terms, the result means that a readiness dashboard based only

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

on linear SEM paths may miss agencies whose readiness depends on interaction effects. For example, strong regulatory legitimacy may compensate for moderate technological capability only when data governance is also strong. Tree-based learners are well suited to identifying such combinations, while SEM provides the conceptual basis for interpreting them.

Explainability analysis reveals that regulatory clarity, data governance, top management support, interoperability readiness, and institutional trust are the most influential features in the hybrid classifier. This ranking is consistent with, but not identical to, the SEM path results. The difference is expected. SEM estimates average structural associations among latent constructs, while feature attribution estimates marginal contribution to predictive classification. A construction can have a moderate SEM path but high predictive importance if it distinguishes agencies near the readiness threshold. Conversely, a construction can have a strong average path but lower predictive importance if most agencies score similarly on it. The explanation stage uses SHAP-style reasoning in line with broader XAI research and the security-focused literature on blockchain-enabled IoT infrastructures (Adadi et al., 2018； Xu et al., 2021).

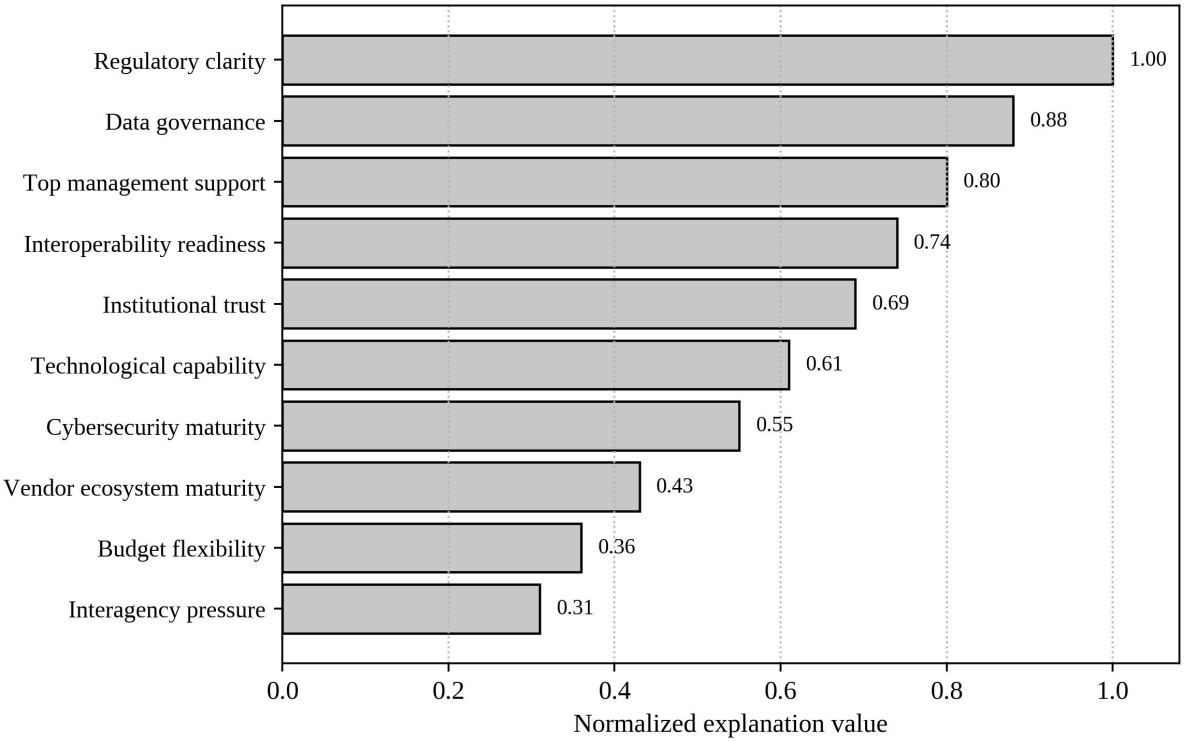

Figure 4. Explainable AI ranking of readiness drivers in the hybrid SEM-machine learning model.

Figure 4 provides a practical explanation layer. The most important feature is regulatory clarity, followed by data governance and top management support. This does not mean that technological capability is unimportant. Rather, the classification task shows that many agencies may possess baseline technical resources, while their readiness is more sharply differentiated by governance and legitimacy conditions. For public managers, this is a critical diagnostic insight. It suggests that blockchain readiness programs should not begin with software procurement alone. They should begin with legal interpretation, data stewardship, executive sponsorship, and an auditable governance model.

VI. READINESS SEGMENTATION AND GOVERNANCE IMPLICATIONS

Beyond binary classification, readiness analytics should support segmentation. Agencies classified as low readiness, transitional

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

readiness, and high readiness require different interventions. A low-readiness agency may need foundational data management, cybersecurity training, and workflow documentation before blockchain is even considered. A transitional agency may need a narrower pilot, stronger legal guidance, or integration standards. A high-readiness agency may be suitable for a controlled pilot if the use case has clear public value, manageable privacy risk, and a credible oversight mechanism. The role of interagency pressure is consistent with technology use research and recent vignette evidence on how public officials evaluate blockchain proposals (Venkatesh et al., 2012； Cagigas et al., 2022).

The segment profile analysis reinforces this point. Low-readiness agencies show negative standardized scores on most constructions, especially data governance and regulatory clarity. Transitional agencies are close to the means on technological capability and management support but below the mean on legitimacy-related conditions. High-readiness agencies show above-average scores across all constructs, with especially strong regulatory clarity and data governance. This pattern indicates that readiness is cumulative. Agencies rarely become high-ready through a single strength. They require a balanced bundle of technical, organizational, and institutional capabilities. The analysis favors intelligible readiness diagnostics because public managers need actionable reasons rather than opaque probability scores (Lou et al., 2012； Zheng et al., 2022).

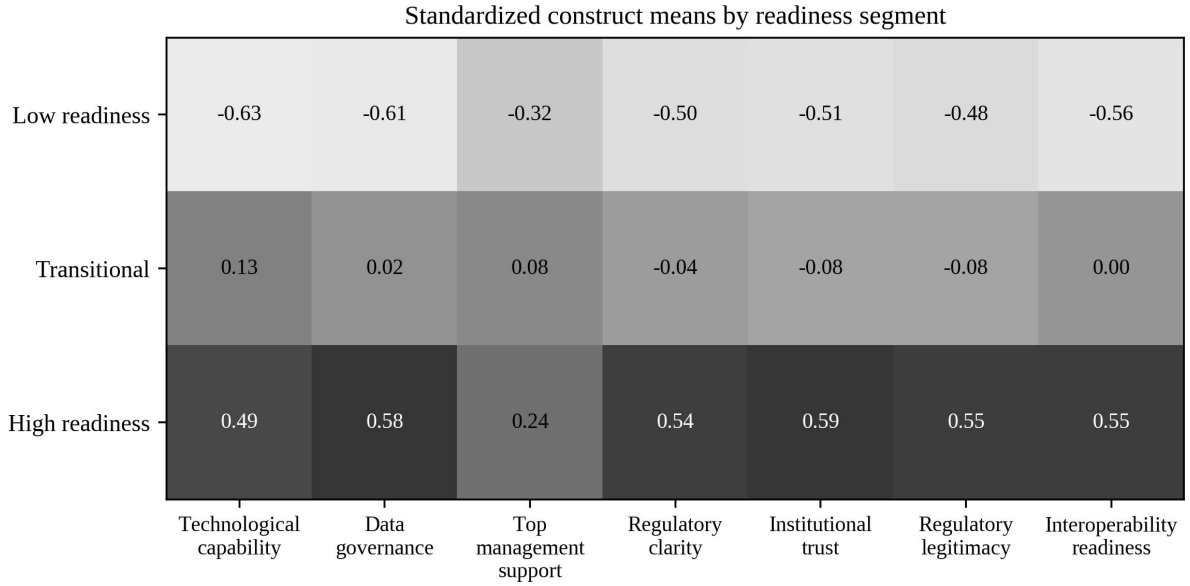

Figure 5. Segment profiles for low, transitional, and high blockchain adoption readiness agencies.

Figure 5 translates the model into a segmentation view. The heatmap shows standardized construction means by readiness group. The main message is that high-readiness agencies are not merely more technically capable; they also have stronger governance, clearer regulatory foundations, and higher institutional trust. This provides a caution against technology-first implementation. In government agencies, readiness should be assessed through a portfolio of conditions that together make adoption defensible, auditable, and sustainable.

Table V. Explainable readiness diagnostics and recommended governance responses.

Dominant barrier identified by XAI	Readiness interpretation	Recommended governance response	Expected public-sector value
Low regulatory clarity	The agency is unsure whether blockchain use is legally authorized or administratively acceptable.	Create legal guidance notes, procurement templates, privacy interpretations, and smart-contract accountability rules.	Reduces legal uncertainty and strengthens legitimacy.
Weak data governance	The agency lacks consistent data ownership, quality	Establish data stewardship roles, metadata standards, retention rules, and error-	Improves reliability of on-chain or off-chain records.

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

	controls, or audit procedures.	correction procedures before pilot design.	
Limited top management support	Blockchain remains an IT experiment without executive sponsorship.	Create a cross-functional steering committee with budget authority, risk oversight, and service-owner representation.	Convert experimentation into accountable organizational commitment.
Low interoperability readiness	Legacy systems and partner agencies cannot exchange reliable data.	Adopt APIs, shared identifiers, data exchange standards, and staged integration testing.	Prevents fragmented pilots and improves interagency coordination.
Low institutional trust	Stakeholders question fairness, competence, or accountability of the proposed system.	Publish governance model, audit rights, fallback procedures, and citizen-facing explanation materials.	Strengthens acceptance and reduces resistance.

Table V demonstrates why explainability is not only a technical feature. In public-sector adoption, explanation creates a bridge between model output and accountable governance. A readiness model may classify an agency as non-ready, but the value of that classification depends on whether managers can understand the reason. If the key barrier is weak data governance, training IT staff in smart contract development will not solve the problem. If the key barrier is regulatory clarity, purchasing a blockchain platform may increase risk rather than reduce it. Explainable readiness diagnostics therefore improve the alignment between analytical evidence and administrative action.

The study also has implications for public value. Blockchain should not be adopted simply because it is modern or because other agencies are piloting it. Public value arises when technology improves transparency, reduces fraud, increases service reliability, protects rights, or lowers coordination costs in ways that conventional architectures cannot achieve as effectively. The hybrid SEM-ML framework supports this assessment by identifying whether an agency has the conditions required to pursue a legitimate public value case. It also highlights when blockchain should be deferred. In some settings, a conventional database with better governance may deliver more value than an under-governed distributed ledger. The article also draws on broad blockchain application reviews and XAI synthesis work to separate technology potential from implementation evidence (Casino et al., 2019； Arrieta et al., 2020). Public-sector interpretation therefore follows evaluation-oriented blockchain governance work that connects ledger design with service effectiveness, administrative capacity, and citizen-facing accountability (Cagigas et al., 2023).

For policymakers, the results suggest a staged readiness program. The first stage should define eligible use cases and legal boundaries. The second should measure agency capability and governance maturity using validated constructions. The third should use explainable predictive analytics to identify readiness segments and capacity-building priorities. The fourth should authorize pilots only when readiness conditions and public value justifications are jointly satisfied. The fifth should require post-implementation monitoring, including auditability, data quality, system resilience, citizen impact, and model explanation logs. This staged approach avoids both technological enthusiasm and excessive caution. The TOE lens is particularly suitable for emerging-economy contexts because adoption barriers often combine resource gaps, partner readiness, and regulatory ambiguity (Chittipaka et al., 2023； Lu, 2019b).

VII. DISCUSSION

The main theoretical implication is that blockchain adoption readiness in government agencies should be understood as an interaction between innovation capability and institutional acceptability. TOE explains why technical, organizational, and environmental factors matter, but institutional theory explains why those factors are filtered through legitimacy and trust. The SEM results support this combined view by showing that regulatory legitimacy is the strongest direct predictor of readiness. The machine learning results extend the argument by showing that regulatory clarity and data governance are among the most influential classification features. Together, these findings show that readiness is not a simple maturity score; it is a multidimensional

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

condition shaped by capability, governance, and legitimacy. Security and interpretability are therefore treated as mutually reinforcing concerns in high-stakes public data infrastructures (Kshetri, 2017； Doshi-Velez et al., 2017).

The study also illustrates methodological contribution. SEM and machine learning are sometimes presented as competing approaches. SEM prioritizes theory, measurement validity, and interpretable path relationships. Machine learning prioritizes predictive accuracy, nonlinear patterns, and classification performance. This article shows that the two approaches can be complementary. SEM can validate the constructs used as inputs, while machine learning can test whether those constructions predict readiness in a decision-relevant way. Explainable AI then connects the two by translating predictive patterns into interpretable diagnostics. The hybrid design is particularly suitable for public-sector analytics because it balances accuracy with accountability. The findings also align with organizational blockchain research showing that top management support, technology competence, and trust shape adoption readiness (Malik et al., 2021； Binns et al., 2018).

The practical implication is that agencies should avoid one-dimensional blockchain readiness assessments. A checklist that asks whether an agency has blockchain developers, cloud infrastructure, and cybersecurity controls is insufficient. A responsible assessment must also ask whether the agency has a valid legal basis, a clear data governance model, leadership commitment, interoperability capacity, and stakeholder trust. The paper's explainable diagnostics show how those factors can be prioritized. The highest-value interventions are not always the most technical ones. Legal guidance, data stewardship, and governance transparency may do more to increase readiness than additional software capability in agencies that already possess baseline IT maturity. The methodological contribution is strengthened by recent work on industrial information integration and systematic mapping of blockchain research gaps (Lu et al., 2023； Yli-Huumo et al., 2016).

The findings are also relevant to vendors and consultants. Public agencies should demand explanations of readiness scores rather than accepting black-box assessments. Vendors should be required to explain which organizational and governance conditions their implementation assumes. Consultants should avoid presenting blockchain as a universal solution and should instead identify situations where distributed ledgers are justified by public value requirements. In this sense, explainable AI can improve procurement quality by making hidden assumptions visible. The discussion of explanations distinguishes faithful model inspection from simplified narratives, a distinction that is especially important when adoption barriers interact (Guidotti et al., 2018； Kouhizadeh et al., 2021).

Finally, the hybrid design advances the idea of evidence-based digital government. Many digital transformation programs depend on narratives of modernization, efficiency, and innovation. Those narratives are not sufficient for high-stakes public infrastructure. Agencies need an architecture of evidence that combines theory, measurement, prediction, explanation, and audit. SEM contributes construct validity, machine learning contributes predictive discrimination, and explainability contributes operational interpretation. When combined, these elements can support more disciplined decisions about when blockchain should be adopted, when it should be postponed, and what capacity-building intervention is most urgent. Auditability is also linked to cybersecurity and accountable-algorithm research, because agencies must document how recommendations are produced and challenged (Lu et al., 2019c； Kroll et al., 2017).

The results also caution against excessive reliance on aggregate readiness scores. A single readiness index may be attractive to senior decision makers, but it can conceal the reason why an agency is ready or not ready. Two agencies may receive the same score for different reasons. One may be constrained by interoperability and legacy integration; another may be constrained by public trust and legitimacy. Explainable AI adds value because it decomposes the score into actionable drivers. In public-sector innovation, this decomposition is essential. It reduces the risk that agencies pursue fashionable pilots while neglecting the institutional work required for responsible adoption. The policy implications extend the supply-chain adoption literature by showing how trust, partner coordination, and interpretability can be translated into government readiness analytics (Queiroz et al., 2019； Rudin, 2019). Broader cybersecurity and frontier-analytics debates further show that blockchain readiness must be evaluated together with secure information integration and emerging

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

computational capabilities (Lu et al., 2019c； Ye et al., 2022).

Another important issue is the relationship between explainability and accountability. Explanations do not automatically make a system accountable. A dashboard that reports that regulatory clarity is the most important readiness driver is useful only if someone has authority to act on that information. The governance model must assign responsibility for legal interpretation, data stewardship, cybersecurity control, vendor oversight, and citizen-facing communication. Without role assignment, explainability becomes descriptive rather than corrective. The proposed hybrid framework therefore should be embedded in an administrative process that links model outputs to accountable decisions, documented rationales, and reviewable follow-up actions. Readiness for scaling is treated as a higher-order capability that includes technology, process, and governance maturity rather than only pilot success (Lu, 2025； Kshetri, 2018).

The framework is also useful for distinguishing readiness for pilots from readiness for scale. A small proof of concept may require only a committed project team and a contained dataset. A scaled public service requires legal authority, cross-agency data agreements, cybersecurity operations, procurement sustainability, service continuity planning, and public communication. The XAI ranking therefore should not be treated as a simple procurement checklist. It should be used as a dynamic governance dashboard that is updated as agencies move from discovery to pilot, from pilot to limited production, and from limited production to institutionalized service delivery. Each stage requires different evidence of readiness. The article therefore warns that explanation interfaces should support accountability, not simply make black-box systems appear more acceptable (Mittelstadt et al., 2019； Dutta et al., 2020).

A further implication concerns the selection of blockchain use cases. Government agencies frequently begin with broad claims about transparency or automation, but the readiness model suggests that use cases should be screened against three questions. First, does the service require multi-party record synchronization in which no single agency can credibly maintain the authoritative record alone? Second, would immutability, shared validation, or programmable rules create a measurable improvement over conventional database modernization? Third, can the agency explain the data lifecycle, error-correction mechanism, citizen rights, and accountability structure before implementation? A proposed blockchain project that fails these questions should be redesigned or deferred, regardless of its predicted technical feasibility. Future work could connect this approach with quantum-era analytics and internal audit frameworks as public agencies modernize financial, identity, and procurement infrastructures (Lu et al., 2024b； Wu et al., 2025).

VIII. LIMITATIONS AND FUTURE RESEARCH

The study has limitations that should be addressed in future work. The most important limitation is that the empirical results are based on a scenario-calibrated synthetic dataset. This design is appropriate for demonstrating the analytical workflow, but it cannot establish country-level or agency-level empirical generalizations. Future research should collect field data from ministries, municipalities, regulatory bodies, and public service agencies across multiple administrative contexts. Such data would allow researchers to test whether the same readiness drivers hold across centralized and decentralized governments, high- and middle-income economies, and different policy domains. This accountability orientation is important because algorithmic auditability depends on records of model development, monitoring, and organizational rights (Raji et al., 2020； Saberi et al., 2019).

A second limitation concerns causality. The SEM paths are consistent with the proposed theoretical logic, but cross-sectional readiness data cannot prove causal effects. Longitudinal studies should track agencies before, during, and after blockchain pilots. Such designs could examine whether improvements in regulatory clarity or data governance increase adoption readiness over time. Quasi-experimental designs may also be possible when governments introduce new digital policies, legal guidance, or funding programs that affect some agencies before others. The contribution also speaks to the broader interpretability literature, where model transparency is valuable only when it supports meaningful human understanding (Carvalho et al., 2019； Ye et al., 2022).

A third limitation concerns explainability evaluation. This article uses model-based feature attribution as an explanation method, but public-sector explainability also requires human evaluation. Future studies should test whether managers, auditors, and

RESEARCH ARTICLE
Vol. 3, No. 3 (2025), pp. 56–74
DOI: 10.63646/jaiaa.2025.030304

citizens understand the explanations, whether explanations increase trust appropriately, and whether they reduce harmful overreliance on automated recommendations. Interpretability should be evaluated as a governance outcome rather than only as a technical property. Blockchain-related logistics research and sociotechnical fairness research both suggest that technical transparency must be embedded in institutional processes (Durach et al., 2021； Selbst et al., 2019).

IX. CONCLUSION

This article developed an explainable AI framework for predicting blockchain adoption readiness in government agencies using a hybrid SEM-machine learning approach. The core argument is that readiness is not merely a technological condition. It is a sociotechnical and institutional condition that combines technical capability, data governance, leadership support, interoperability, regulatory clarity, institutional trust, and regulatory legitimacy. The structural results identify regulatory legitimacy, technological capability, top management support, data governance, and institutional trust as central readiness drivers. The predictive results show that a hybrid SEM-ML model outperforms single-method classifiers in identifying high-readiness agencies. The limitations section therefore treats explanations as contestable artifacts, because explanation methods can be manipulated or misunderstood in practice.

The broader contribution is practical and normative. Government agencies should not use AI readiness scores unless those scores can be explained, challenged, and translated into accountable action. The explainability results show that regulatory clarity, data governance, top management support, interoperability readiness, and institutional trust are the most actionable diagnostic areas. A public agency that wants to adopt blockchain responsibly should therefore begin with governance architecture, legal clarity, data stewardship, and public value justification. Blockchain adoption becomes defensible only when technical possibility is matched by institutional legitimacy and transparent accountability. For government agencies, the governance risk is especially salient because automated readiness ratings can influence procurement, budget allocation, and interagency priorities.

AUTHOR CONTRIBUTIONS

Author	Contribution
Amina Rahman	Conceptualization, methodology, writing - original draft, visualization
Daniel Lim	Formal analysis, data curation, validation, writing - review and editing
Farah Sulaiman	Supervision, project administration, governance analysis, writing - review and editing

DECLARATIONS

Conflicts of interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

Data availability: The empirical analysis uses a scenario-calibrated synthetic dataset generated for methodological demonstration. No proprietary government dataset or identifiable personal record is redistributed in this manuscript.

Funding: This research received no external funding.

Ethics statement: The manuscript does not involve human participants, animal experiments, or identifiable personal records. A future field study using real agency respondents would require institutional ethics approval and administrative permission before data collection.

ABOUT THE AUTHORS

Amina Rahman is affiliated with the Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Malaysia. Her research focuses on explainable machine learning, data governance, and public-sector digital

transformation.

Daniel Lim is affiliated with the Faculty of Business and Management, Universiti Teknologi MARA, Malaysia. His research interests include technology adoption, digital government innovation, and organizational analytics.

Farah Sulaiman is affiliated with the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia. Her research addresses AI governance, blockchain-enabled information systems, and accountable public-service innovation.

REFERENCES

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

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

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. https://doi.org/10.2307/30036540

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

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. https://doi.org/10.1080/07421222.2003.11045748

Cagigas, D., Clifton, J., Díaz-Fuentes, D., & Fernández-Gutiérrez, M. (2021). Blockchain for public services: A systematic literature review. IEEE Access, 9, 13904-13921. https://doi.org/10.1109/ACCESS.2021.3052019

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. Psychological Bulletin, 103(3), 411-423. https://doi.org/10.1037/0033-2909.103.3.411

Kamble, S. S., Gunasekaran, A., Kumar, V., Belhadi, A., & Foropon, C. (2021). A machine learning based approach for predicting blockchain adoption in supply chain. Technological Forecasting and Social Change, 163, 120465. https://doi.org/10.1016/j.techfore.2020.120465

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why should I trust you? Explaining the predictions of any classifier. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135-1144. https://doi.org/10.1145/2939672.2939778

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

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

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, Article 76. https://doi.org/10.1145/3209281.3209317

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39-50. https://doi.org/10.2307/3151312

Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. Advances in Neural Information Processing Systems, 30. https://doi.org/10.48550/arXiv.1705.07874

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. https://doi.org/10.1007/s10796-022-10248-7

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

Falwadiya, H., & Dhingra, S. (2022). Blockchain technology adoption in government organizations: A systematic literature review. Journal of Global Operations and Strategic Sourcing, 15(3), 473-501. https://doi.org/10.1108/JGOSS-09-2021-0079

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling, 6(1), 1-55. https://doi.org/10.1080/10705519909540118

Breiman, L. (2001). Random forests. Machine Learning, 45, 5-32. https://doi.org/10.1023/A:1010933404324

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. https://doi.org/10.1080/17517575.2024.2448003

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51-90. https://doi.org/10.2307/30036519

Cagigas, D., Clifton, J., Díaz-Fuentes, D., Fernández-Gutiérrez, M., Echevarría-Cuenca, J., & Gilsanz-Gómez, C. (2022). Explaining public officials' opinions on blockchain adoption: A vignette experiment. Policy and Society, 41(3), 343-357. https://doi.org/10.1093/polsoc/puab022

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43, 115-135. https://doi.org/10.1007/s11747-014-0403-8

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 785-794. https://doi.org/10.1145/2939672.2939785

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. https://doi.org/10.1080/17517575.2024.2397630

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. https://doi.org/10.1287/isre.13.3.334.81

Lykidis, I., Drosatos, G., & Rantos, K. (2021). The use of blockchain technology in e-government services. Computers, 10(12), 168. https://doi.org/10.3390/computers10120168

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. Journal of the Academy of Marketing Science, 40, 414-433. https://doi.org/10.1007/s11747-011-0261-6

Friedman, J. H. (2001). Greedy function approximation: A gradient boosting machine. Annals of Statistics, 29(5), 1189-1232. https://doi.org/10.1214/aos/1013203451

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

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. https://doi.org/10.2307/30036550

Saxena, S., Shao, D., Ṇikiforova, A., & Thapliyal, R. (2022). Invoking blockchain technology in e-government services: A cybernetic perspective. Digital Policy, Regulation and Governance, 24(3), 246-258. https://doi.org/10.1108/DPRG-10-2021-0128

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879-903. https://doi.org/10.1037/0021-9010.88.5.879

Geurts, P., Ernst, D., & Wehenkel, L. (2006). Extremely randomized trees. Machine Learning, 63, 3-42. https://doi.org/10.1007/s10994-006-6226-1

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

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

Bustamante, P., Cai, M., Gomez, M., Harris, C., Krishnamurthy, P., Law, W., Madison, M. J., Murtazashvili, I., Murtazashvili, J. B., Mylovanov, T., Shapoval, N., Vee, A., & Weiss, M. (2022). Government by code? Blockchain applications to public sector governance. Frontiers in Blockchain, 5, 869665. https://doi.org/10.3389/fbloc.2022.869665

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of sustainable enterprise performance. Strategic Management Journal, 28(13), 1319-1350. https://doi.org/10.1002/smj.640

Guan, W., Ding, W., Zhang, B., Verny, J., & Hao, R. (2023). Do supply chain related factors enhance the prediction accuracy of blockchain adoption? A machine learning approach. Technological Forecasting and Social Change, 192, 122552. https://doi.org/10.1016/j.techfore.2023.122552

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

Zhu, K., Kraemer, K. L., & Xu, S. (2006). The process of innovation assimilation by firms in different countries: A technology diffusion perspective on e-business. Management Science, 52(10), 1557-1576. https://doi.org/10.1287/mnsc.1050.0487

Wamba, S. F., Wamba-Taguimdje, S.-L., Lu, Q., & Queiroz, M. M. (2024). How emerging technologies can solve critical issues in organizational operations: An analysis of blockchain-driven projects in the public sector. Government Information Quarterly, 41(1), 101912. https://doi.org/10.1016/j.giq.2024.101912

Saito, T., & Rehmsmeier, M. (2015). The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets. PLOS ONE, 10(3), e0118432. https://doi.org/10.1371/journal.pone.0118432

Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). IEEE Access, 6, 52138-52160. https://doi.org/10.1109/ACCESS.2018.2870052

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. https://doi.org/10.1109/JIOT.2021.3060508

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1), 157-178. https://doi.org/10.2307/41410412

Cagigas, D., Clifton, J., Díaz-Fuentes, D., Fernández-Gutiérrez, M., & Harpes, C. (2023). Blockchain in government: Toward an evaluation framework. Policy Design and Practice, 6(4), 397-414. https://doi.org/10.1080/25741292.2023.2230702

Lou, Y., Caruana, R., & Gehrke, J. (2012). Intelligible models for classification and regression. Proceedings of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 150-158. https://doi.org/10.1145/2339530.2339556

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

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

Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82-115. https://doi.org/10.1016/j.inffus.2019.12.012

Chittipaka, V., Kumar, S., Sivarajah, U., Bowden, J. L.-H., & Baral, M. M. (2023). Blockchain technology for supply chains operating in emerging markets: An empirical examination of the technology-organization-environment framework. Annals of Operations Research, 327(1), 465-492. https://doi.org/10.1007/s10479-022-04801-5

Lu, Y. (2019b). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1-29. https://doi.org/10.1080/23270012.2019.1570365

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

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv. https://doi.org/10.48550/arXiv.1702.08608

Malik, S., Chadhar, M., Vatanasakdakul, S., & Chetty, M. (2021). Factors affecting the organizational adoption of blockchain technology: Extending the technology-organization-environment framework in the Australian context. Sustainability, 13(16), 9404. https://doi.org/10.3390/su13169404

Binns, R., Van Kleek, M., Veale, M., Lyngs, U., Zhao, J., & Shadbolt, N. (2018). It's reducing a human being to a percentage: Perceptions of justice in algorithmic decisions. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1-14. https://doi.org/10.1145/3173574.3173951

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. https://doi.org/10.1016/j.jii.2023.100511

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. https://doi.org/10.1371/journal.pone.0163477

Guidotti, R., Monreale, A., Ruggieri, S., Turini, F., Giannotti, F., & Pedreschi, D. (2018). A survey of methods for explaining black box models. ACM Computing Surveys, 51(5), Article 93. https://doi.org/10.1145/3236009

Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. International Journal of Production Economics, 231, 107831. https://doi.org/10.1016/j.ijpe.2020.107831

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

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165(3), 633-705. https://doi.org/10.2139/ssrn.2765268

Queiroz, M. M., & Wamba, S. F. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. International Journal of Information Management, 46, 70-82. https://doi.org/10.1016/j.ijinfomgt.2018.11.021

Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nature Machine Intelligence, 1(5), 206-215. https://doi.org/10.1038/s42256-019-0048-x

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

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

Mittelstadt, B., Russell, C., & Wachter, S. (2019). Explaining explanations in AI. Proceedings of the Conference on Fairness, Accountability, and Transparency, 279-288. https://doi.org/10.1145/3287560.3287574

Dutta, P., Choi, T.-M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation Research Part E: Logistics and Transportation Review, 142, 102067. https://doi.org/10.1016/j.tre.2020.102067

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

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 33-44. https://doi.org/10.1145/3351095.3372873

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. https://doi.org/10.1080/00207543.2018.1533261

Carvalho, D. V., Pereira, E. M., & Cardoso, J. S. (2019). Machine learning interpretability: A survey on methods and metrics. Electronics, 8(8), 832. https://doi.org/10.3390/electronics8080832

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

Durach, C. F., Blesik, T., von Düring, M., & Bick, M. (2021). Blockchain applications in supply chain transactions. Journal of Business Logistics, 42(1), 7-24. https://doi.org/10.1111/jbl.12238

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. Proceedings of the Conference on Fairness, Accountability, and Transparency, 59-68. https://doi.org/10.1145/3287560.3287598

Slack, D., Hilgard, S., Jia, E., Singh, S., & Lakkaraju, H. (2020). Fooling LIME and SHAP: Adversarial attacks on post hoc explanation methods. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 180-186. https://doi.org/10.1145/3375627.3375830

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

Veale, M., & Brass, I. (2019). Administration by algorithm? Public management meets public sector machine learning. In K. Yeung & M. Lodge (Eds.), Algorithmic Regulation (pp. 121-149). Oxford University Press. https://doi.org/10.1093/oso/9780198838494.003.0006

Wachter, S., Mittelstadt, B., & Russell, C. (2017). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. Harvard Journal of Law & Technology, 31(2), 841-887. https://doi.org/10.2139/ssrn.3063289