

Integrating Information Systems Success, Institutional, and Resource Dependence Theories for Blockchain-Based Health Interoperability in LMICs

Peter M. Halwenge^{1*}, Hesborn O. Nyagowa¹, Caroline N. Musembe¹

¹*The Technical University of Kenya, P.O BOX 52428-00100, Nairobi-Kenya*

*Correspondence email: halwengems@gmail.com

Abstract

Digital health interoperability in devolved public health systems is constrained by technical, organisational, and systemic factors that current research treats as competing rather than complementary diagnoses. This paper asks which theoretical lens should govern a given readiness question, and answers through a four-step theoretical conceptual synthesis: selecting five established lenses, the DeLone and McLean Information Systems Success Model, the Blockchain Trilemma, the Parkerian Hexad, Institutional Theory, and Resource Dependence Theory; constructing an integrating structure; analysing tension and complementarity between lenses; and illustrating the resulting framework against a real governance context. Readiness is defined as the joint sufficiency of a health system's technical capacity, organisational legitimacy, and source-system quality to support a blockchain interoperability layer. The five lenses are organised along three readiness dimensions: technical, organisational, and systemic and applied to Kenya's devolved health system, including county-level evidence from Kisumu, drawing on the Constitution of Kenya (2010), the Digital Health Act (2023), the Kenya Health Information Systems Interoperability Framework (2020), the Data Protection Act (2019), and published accounts of electronic medical record fragmentation. Benchmarked against the WHO-ITU National eHealth Strategy Toolkit, the framework is shown to add diagnostic precision that a single-lens or purely strategic instrument does not supply. We conclude that treating readiness as one undifferentiated construct risks misdiagnosing which intervention a context actually needs, and recommend that certification regimes, research instruments, and technical-assistance programmes test technical, organisational, and systemic readiness separately rather than assuming the three co-vary.

Keywords: *blockchain interoperability, health information systems, institutional theory, resource dependence theory,*

IJPP 14(6); 76-91

1.0 Introduction

Interest in blockchain as an interoperability layer for fragmented health information systems has grown quickly across low- and middle-income countries (LMICs), producing a steady stream of proposed architectures, pilot deployments, and readiness assessments. What has grown more slowly is theoretical coherence. Individual studies typically borrow a single lens, a technology adoption model to explain use intention, a security taxonomy to specify technical controls, or an engineering trade-off theorem to justify an architectural choice without placing that lens alongside the others operating on the same phenomenon. The result is a literature that is empirically active but theoretically fragmented: findings from a security-focused study and findings from an organisational-behaviour study are rarely read as complementary evidence about the same underlying readiness construct.

This pattern is evident in recent single-lens studies. Kore et al. (2026), for example, examine blockchain readiness in two Ethiopian hospitals primarily through a technology-adoption and organisational-readiness perspective. Their findings indicate that positive staff attitudes do not necessarily translate into institutional preparedness, but they do not examine whether the observed shortfall might also reflect security limitations, institutional legitimacy pressures, or upstream data-quality problems. Isemeck et al. (2019) explain uneven electronic health record (EHR) adoption in public health facilities in Kisumu County largely in techno-organisational terms without situating the findings within the security requirements of the data that would ultimately be exchanged. Similarly, Joshi and Sharma (2023) identify implementation barriers to blockchain in public healthcare in developing countries primarily in terms of infrastructure and security while treating organisational legitimacy as a secondary consideration. Each study provides a useful explanation of a particular aspect of the problem, but none

explicitly distinguishes whether the identified constraint is technical, organisational, or systemic, or whether several constraints may operate simultaneously.

It is therefore no surprise that empirical investigation of health care organisations' readiness to deploy blockchain technologies remains scarce, and that the few published assessments are confined to single facilities or single national settings (Joshi & Sharma, 2023; Kore et al., 2026). A policymaker or systems architect reading the blockchain-health literature will encounter technical prescriptions (such as secure the exchange layer), organisational prescriptions (for example, build institutional capacity), and systemic prescriptions (for example, fix the underlying data quality) as if these were competing rather than complementary diagnoses. Since there is little in the way of an organising framework or structure that integrates the multiple dimensions of readiness, it is also very difficult to determine which prescription applies to a given deployment context, or whether more than one constraint is binding at the same time.

"This paper has integrated five theoretical lenses spanning technical, organisational, and systemic dimensions into a single conceptual framework for blockchain health interoperability readiness in LMIC settings."

For the purposes of this paper, readiness is defined as the joint sufficiency of a health system's technical capacity, organisational legitimacy, and source-system quality to support a blockchain interoperability layer. A

health system is therefore not simply ready or unready. Rather, it may demonstrate different levels of readiness across three dimensions that can vary independently. This definition leads to the central question guiding the paper: Which theoretical lens should a researcher or policymaker use to determine the dimension of readiness that is binding in a particular deployment context, and how do the different lenses relate to one another when integrated into a single framework? Answering this question, rather than adding another single-lens study to the literature, constitutes the specific objective of this paper.

Five theoretical lenses, each previously used separately to describe some aspect of blockchain health interoperability, are brought together to pursue that objective. The DeLone and McLean Information Systems Success Model traces how system, information, and service quality determine use and net benefits. The Blockchain Trilemma describes the engineering trade-off among decentralisation, security, and scalability that any ledger architecture must resolve. The Parkerian Hexad, less familiar outside information-security circles, extends the standard confidentiality-integrity-availability triad with three further properties, possession or control, authenticity, and utility to give a fuller account of what a secure data exchange layer must preserve. Institutional Theory explains why formal compliance structures can decouple from day-to-day operational practice under legitimacy pressure. Resource Dependence Theory explains why organisations orient their behaviour, including their documentation practices, toward whoever controls the resources they depend on.

Rather than presenting these perspectives as an inventory of unrelated theories, the paper integrates them across three dimensions of readiness: technical, organisational, and systemic. The framework is then illustrated using Kenya's devolved health system, including sub-national evidence from Kisumu County. The analysis relies on publicly

documented institutional and policy conditions rather than primary survey or interview data. Primary quantitative, qualitative, and Delphi-validated evidence associated with a related interoperability framework is reported separately in the companion doctoral study by Halwenge (2026).

The fragmentation problem in blockchain-health theory

Systematic reviews of blockchain applications in healthcare identify two patterns that are particularly relevant to the present study (Joshi & Sharma, 2023; Kore et al., 2026). First, many proposed frameworks remain conceptual or at the prototype stage and are evaluated against generic adoption or security criteria rather than against the infrastructural and institutional conditions of the settings in which they are intended to operate. Second, where theory is invoked, it is commonly applied through a single lens: technology acceptance or information systems models to explain intended use, security taxonomies to specify technical controls, or organisational theories to explain implementation failures after they occur rather than to inform readiness assessment before implementation.

The consequence is that the same empirical observation for example, a health facility that scores highly on formal readiness documentation but demonstrates limited operational change can be interpreted differently depending on the theoretical perspective adopted. A technology-adoption perspective may describe the situation as an attitude-behaviour gap; a security perspective may consider the observation largely irrelevant because documentation is not itself a security property; and an organisational perspective may identify it as an example of institutional decoupling. Each interpretation may be valid within its own theoretical domain. What is missing is a framework that specifies, in advance, which lens should be applied to which class of observation and how the resulting diagnoses should be related.

The sections that follow develop such a framework.

2.0 Materials and Methods

This paper adopts a theoretical conceptual synthesis approach appropriate for research whose contribution is the integration of previously separate theoretical traditions rather than the generation of new primary data. Consistent with recognised conceptual research designs, the study proceeds in four steps: (a) selection of candidate theoretical lenses, (b) construction of an integrating structure that maps the lenses onto distinct dimensions of the target construct, (c) analysis of the points of tension and complementarity between lenses, and (d) illustrative application of the resulting framework to a real-world governance context using publicly available documentary sources.

Selection of theoretical lenses

Five lenses were purposively selected on the basis of three criteria. First, each lens had to have been used, in prior peer-reviewed literature, to explain some aspect of blockchain-based interoperability or, more broadly, health information system readiness. Second, the lenses collectively had to span the technical, organisational, and systemic domains identified in earlier reviews of blockchain implementation in health care as the recurrent sites of implementation constraint (Joshi & Sharma, 2023). Third, the lenses had to differ sufficiently in their disciplinary origin so that their integration would extend, rather than merely restate, existing theoretical treatments. The five lenses that met these criteria were the DeLone and McLean Information Systems Success Model, the Blockchain Trilemma, the Parkerian Hexad, Institutional Theory (particularly the concept of decoupling as developed by Meyer and Rowan, and by DiMaggio and Powell), and Resource Dependence Theory as developed by Pfeffer and Salancik.

Framework construction

For each selected lens, the paper first restates the lens in its original form and identifies its core proposition. The lens is then translated to the specific empirical target of blockchain interoperability readiness, in a manner that preserves its original theoretical claim while making its predictions concrete for the target context. Each lens is then assigned to one of three readiness dimensions, technical, organisational, or systemic on the basis of the type of readiness constraint it is best positioned to explain. Where two lenses occupy the same dimension, the paper specifies the division of theoretical labour between them, so that each lens addresses a distinct aspect of the constraint rather than duplicating the other.

Analysis of tension and complementarity

Rather than treat the five lenses as simply additive, the paper analyses pairs in which productive tension or overlap arises and specifies how the integrated framework resolves that tension distinguishing a genuine theoretical integration from a mere theoretical inventory.

Document selection for the illustrative application

Two categories of publicly available document were used to illustrate the framework, selected purposively rather than through a systematic review, since the aim is to demonstrate how the framework organises existing evidence rather than to establish new empirical findings. The first category comprises the complete set of national statutory and policy instruments currently governing digital health interoperability under Kenya's devolved constitutional arrangement: the Constitution of Kenya (2010), the National eHealth Policy 2016–2030, the Kenya Health Information Systems Interoperability Framework (2020), the Data Protection Act (2019), the Digital Health Act (2023), and the Digital Health (Health Information Management Procedures) Regulations (2025). These six instruments were not sampled from a larger population; they are,

at the time of writing, the exhaustive set of binding national instruments addressing health-data interoperability, and the selection criterion was simply that each instrument sets requirements a blockchain interoperability layer would need to satisfy. The second category comprises peer-reviewed, publicly available empirical studies describing the electronic health record landscape of one specific county, Kisumu, selected because it is both the site of Kenya's first pilot of the national Electronic Community Health Information System and the subject of several independent published assessments of electronic medical record fragmentation (Ireru et al., 2025; Isemeck et al., 2019; Juma et al., 2020). No primary data are used in this paper; the corresponding quantitative, qualitative, and Delphi-validated evidence for a related interoperability framework is reported in a companion doctoral study by the author (Halwenge, 2026). The illustrative application is intended to demonstrate how the present framework functions as a diagnostic instrument, not to make new empirical claims about any Kenyan county.

Benchmarking against an existing framework

To situate the framework's contribution relative to existing instruments, its structure is compared against the WHO-ITU National eHealth Strategy Toolkit (World Health Organization & International Telecommunication Union, 2012), the most widely adopted international reference for national eHealth strategy development and the basis for subsequent continental assessment tools (Olufadewa et al., 2024). The comparison, reported in the next section, asks what the toolkit and the present framework each treat as the unit of readiness, and what each would recommend for a county exhibiting the same evidence.

Limitations of the conceptual approach

Because this paper is conceptual rather than empirical, the integrated framework itself has not been subjected to expert review, Delphi

validation, or pilot testing, and its diagnostic claims should be read as propositions for testing rather than as established findings. A structured expert-validation exercise, modelled on the Delphi procedure used to validate a related interoperability framework in the author's companion doctoral study (Halwenge, 2026), is identified in the Recommendations section as the appropriate next step.

Ethical considerations

This paper analyses no primary human-subjects data and therefore did not itself require research ethics review. Ethical reflexivity nonetheless applies to conceptual work intended to inform health data governance policy: the paper draws only on sources already in the public domain, none of the cited county-level studies discloses individually identifiable patient information, and the framework's illustrative application is presented explicitly as diagnostic rather than evaluative, so that no county, facility, or official is characterised as non-compliant on the strength of publicly available documents alone. The companion empirical study from which primary quantitative, qualitative, and Delphi data are drawn separately received ethical approval from the Jaramogi Oginga Odinga Ethical Review Board and a research licence from the Kenya National Commission for Science, Technology and Innovation (Halwenge, 2026).

3.0 Results and Discussions

The theoretical synthesis produced three principal results: (a) a translation of each of the five selected lenses into a proposition about blockchain interoperability readiness; (b) an integrated framework organising the five lenses along three readiness dimensions; and (c) an illustrative application of the framework to Kenya's devolved health governance context that identifies which dimension of readiness is binding under which set of empirical conditions. These results are presented and discussed in an integrated flow below.

The five theoretical lenses

DeLone and McLean Information Systems Success Model

The DeLone and McLean model proposes that system quality, information quality, and service quality influence use and user satisfaction, which subsequently contribute to net benefits (DeLone & McLean, 2003). Applied to blockchain interoperability, the model highlights the importance of the quality of the information systems that exist beneath the blockchain layer.

A blockchain interoperability layer cannot automatically correct deficiencies in the source systems from which data originate. If EHR systems generate incomplete, inconsistent, inaccurate, or poorly structured information, the blockchain layer may preserve and exchange those deficiencies rather than eliminate them. Consequently, source-system quality should be considered a fundamental component of interoperability readiness rather than a secondary issue to be addressed after blockchain implementation.

This interpretation is consistent with recent applications of the DeLone and McLean model to EHR-related outcomes, including medical-error reduction (Chimbo & Motsi, 2024). In the context of the present framework, the principal theoretical implication is therefore that source-system quality is logically prior to successful interoperability

Blockchain Trilemma

The Blockchain Trilemma describes the engineering trade-off among decentralisation, security, and scalability (Zhou et al., 2020). Blockchain architectures cannot generally maximise all three properties simultaneously. Increasing decentralisation may introduce performance and governance challenges, while increasing security and scalability may require greater centralisation or controlled participation.

This trade-off is particularly important in national and sub-national health systems

operating under infrastructure constraints. A fully decentralised and open architecture may not provide the performance, governance, or assurance required for health information exchange at scale. The trilemma therefore provides a technical lens for evaluating alternative architectures and may support consideration of permissioned or consortium-based blockchain arrangements in which participating health authorities and other authorised entities operate under defined governance rules.

The trilemma does not prescribe a single architecture. Rather, it requires architecture choices to be justified explicitly in relation to the competing requirements of decentralisation, security, and scalability

Parkerian Hexad

The Parkerian Hexad extends the conventional confidentiality-integrity-availability security triad by adding possession or control, authenticity, and utility (Parker, 2014). Applied to health-information exchange, the hexad provides six properties against which an interoperability architecture can be assessed.

The Hexad is complementary to the Blockchain Trilemma. Whereas the trilemma addresses architecture-level trade-offs, the Parkerian Hexad specifies information-security properties that the selected architecture should preserve. The two lenses therefore operate at different levels of technical analysis: the trilemma informs architectural choice, while the Hexad informs security-property assessment

Institutional Theory

Institutional Theory, particularly the concept of institutional decoupling, explains why formal organisational structures, policies, procedures, and compliance artefacts may diverge from actual operational practices (Meyer & Rowan, 1977; DiMaggio & Powell, 1983). Such divergence may occur when organisations face strong external pressures to demonstrate

legitimacy to regulators, funders, professional bodies, or other stakeholders.

Applied to health-system readiness, institutional theory suggests that documentation-based assessments may overestimate operational readiness where organisations can produce formal compliance artefacts without possessing equivalent operational capacity. Readiness assessments based exclusively on policies, plans, reports, or self-reported indicators may therefore fail to distinguish formal compliance from actual implementation capacity.

Institutional theory consequently constitutes the principal organisational lens for explaining the potential gap between documented readiness and operational readiness.

Resource Dependence Theory

Resource Dependence Theory holds that organisations adapt their behaviour in response to external actors that control resources critical to their survival (Pfeffer & Salancik, 1978). In devolved health systems, sub-national governments may depend on national transfers, donor funding, technical assistance, infrastructure support, and other external resources.

Applied to blockchain interoperability readiness, the theory suggests that county-level organisations may orient their reporting, planning, and documentation practices toward the expectations of actors controlling critical resources. The production of readiness documentation may therefore reflect not only internal capacity but also the external resource environment within which an organisation operates.

Resource Dependence Theory complements Institutional Theory by explaining whose expectations organisations may seek to satisfy. Institutional theory helps explain why formal structures may become decoupled from operational practice, whereas Resource Dependence Theory helps explain how

dependence on external resource controllers shapes organisational behaviour

Points of tension and complementarity

The five lenses are not simply additive; some sit in productive tension. Institutional theory's emphasis on legitimacy-seeking behaviour and resource dependence theory's emphasis on resource-seeking behaviour can, in a given empirical instance, offer competing explanations for the same organisational behaviour for example, whether a county produces a sustainability plan primarily to appear legitimate to peer institutions or primarily to satisfy the specific reporting requirements of a donor. The two theories are compatible rather than contradictory: legitimacy and resource access are frequently pursued through the same formal artefacts, particularly where the resource controller is also positioned as a legitimacy-conferring authority, as national ministries or multinational donors typically are.

A second point of tension sits between the technical-dimension lenses and the systemic-dimension lens. The blockchain trilemma and the Parkerian Hexad both presuppose a source-system environment capable of producing reliable, well-formed data for the ledger to secure and exchange. Where the DeLone and McLean model's quality preconditions are not met upstream, technical-dimension interventions, however well designed cannot compensate; this is the theoretical basis for treating systemic (source-system) quality as logically prior to technical (ledger-layer) design decisions, rather than as a parallel workstream.

An integrated framework

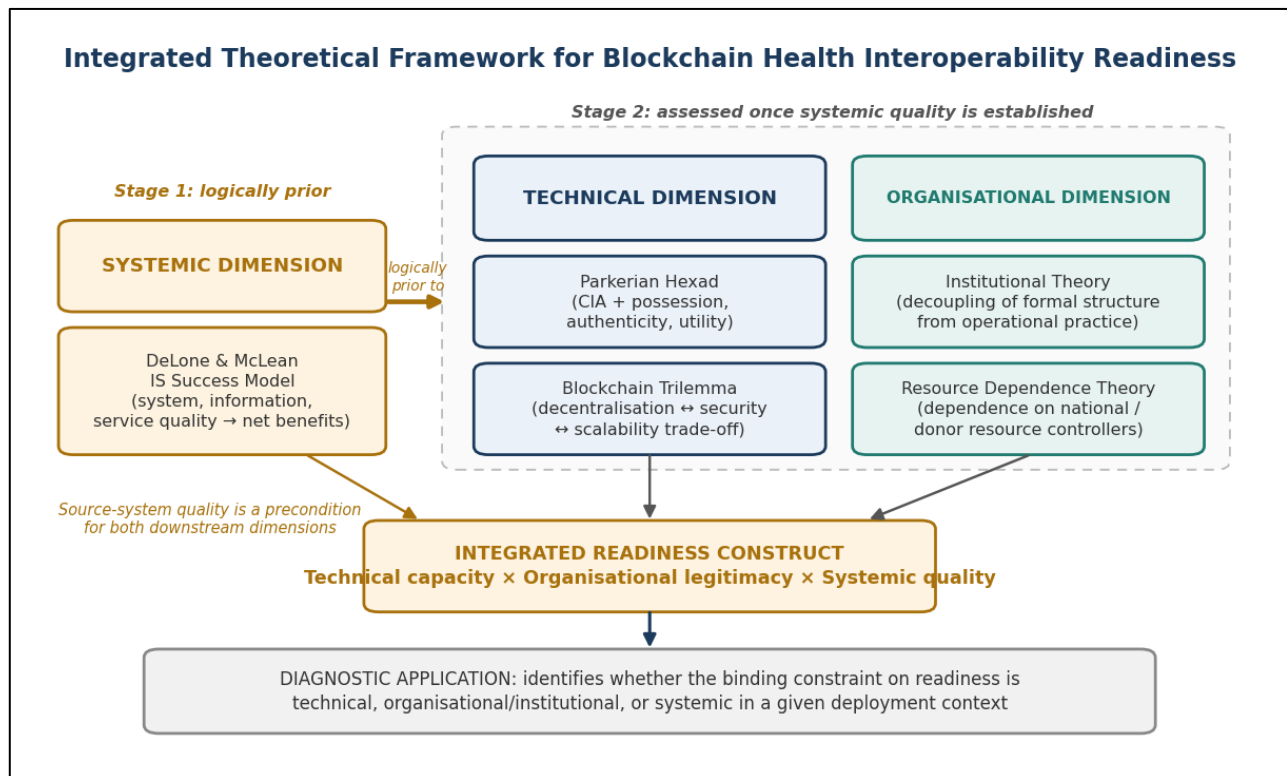
Figure 1 organises the five lenses along three dimensions, technical, organisational, and systemic that jointly determine an integrated readiness construct. The technical dimension (Parkerian Hexad, Blockchain Trilemma) addresses what the exchange layer must be capable of and what trade-offs its architecture must resolve. The organisational dimension (Institutional Theory, Resource Dependence

Theory) addresses how the organisations operating within the health system will behave under legitimacy and resource pressures, including how faithfully their documented capacity will track their operational capacity.

The systemic dimension (DeLone and McLean IS Success Model) addresses the quality of the source-system environment on which the entire interoperability effort depends.

Figure 1

Integrated theoretical framework mapping five theoretical lenses onto technical, organisational, and systemic dimensions of blockchain health interoperability readiness



Note. The framework maps each of five theoretical lenses onto one of three readiness dimensions. The systemic dimension is depicted as Stage 1 and as logically prior to the technical and organisational dimensions (Stage 2), since upstream source-system data quality is a precondition for both technical exchange and organisational reporting. The three dimensions then combine into an integrated readiness construct that is applied diagnostically to identify which constraint is binding in a given context.

The framework depicted in Figure 1 is a proposed diagnostic instrument assembled from previously validated component theories; the integration itself has not undergone independent expert or empirical validation, a limitation addressed directly later in this section.

Table 1 restates this mapping in tabular form, adding the core proposition each lens contributes to the integrated construct.

Table 1

Theoretical grounding matrix: lens, dimension, and core proposition applied

Theoretical lens	Dimension addressed	Core proposition applied
DeLone & McLean IS Success Model	Systemic	System, information, and service quality influence use and net benefits; a blockchain layer inherits the quality of the source systems beneath it and cannot automatically correct upstream data-quality deficiencies.
Blockchain Trilemma	Technical	Decentralisation, security, and scalability involve competing architectural priorities that cannot generally be maximised simultaneously; infrastructure and governance constraints therefore require explicit architectural trade-offs.
Parkerian Hexad	Technical	Confidentiality, integrity, availability, possession/control, authenticity, and utility provide six security properties against which a health-information exchange architecture can be assessed.
Institutional Theory	Organisational	Formal structures and documented compliance may become decoupled from operational practice under legitimacy pressure, meaning that documented readiness does not necessarily demonstrate operational readiness.
Resource Dependence Theory	Organisational	Organisations adapt behaviour toward external actors controlling critical resources, helping explain how national and donor expectations can shape county-level planning, reporting, and readiness documentation.

Note. Each row summarises one theoretical lens, the readiness dimension to which it contributes, and the core proposition it supplies to the integrated framework depicted in Figure 1.

Illustrative application: Kenya's devolved health system

Kenya's devolved health system provides a useful context in which to demonstrate the potential application of the integrated framework. Its constitutional, legislative, and administrative arrangements address technical, organisational, and systemic issues relevant to blockchain-based health-information interoperability.

The application is illustrative rather than empirical. It relies on publicly available statutory instruments, national policy documents, and published empirical studies and does not use primary survey, interview, or Delphi data. The associated primary evidence is reported separately in Halwenge (2026).

Constitutional and policy architecture

Article 43(1)(a) of the Constitution of Kenya (2010) guarantees the right to the highest attainable standard of health. The Fourth Schedule distributes health responsibilities between the national and county governments. County governments are responsible for county health services, including county health facilities and pharmacies, ambulance services, and promotion of primary healthcare, while the national government retains responsibility for health policy, national referral facilities, and capacity building and technical assistance to counties.

The Health Act, No. 21 of 2017, further requires county governments to implement national health policy and standards. This dual

Halwenge, Nyagowa & Musembe

governance structure means that county governments operate under varying financial, infrastructural, and human-resource conditions while remaining subject to national requirements relating to health information and interoperability.

Several subsequent instruments have shaped Kenya's digital-health governance environment. The National eHealth Policy 2016–2030 identified integration and interoperability of health information systems as national priorities (Kenya Ministry of Health, 2016). The Kenya Health Information Systems Interoperability Framework established standards for technical and semantic interoperability among health information systems (Kenya Ministry of Health, 2020).

The Data Protection Act, No. 24 of 2019 established a general legal framework for the processing of personal data, including health information, and established the Office of the Data Protection Commissioner. The Digital Health Act, No. 15 of 2023 established a Digital Health Agency and provided for the development of a Comprehensive Integrated Health Information System (CIHIS) as part of the national digital-health architecture. The Digital Health (Health Information Management Procedures) Regulations, 2025 subsequently provided additional requirements concerning digital-health information management and certification.

This layered combination of constitutional devolution, health-sector policy, data-protection legislation, and digital-health legislation creates a governance environment in which technical, organisational, and systemic readiness can be examined as distinct but interconnected dimensions.

Applying the systemic dimension

The systemic dimension directs attention to the quality of the source-system environment that any interoperability layer inherits. Every county has its own electronic health record ecosystem, shaped by past donor investment in health

information systems, differences in county fiscal capacity, and differences in how consistently staff have been retained over time. The Kenya Health Information Systems Interoperability Framework (Kenya Ministry of Health, 2020) tacitly recognises this variation in source-system quality, but it does not address what should happen where source systems are absent, paper-based, or incomplete.

Kisumu County offers a concrete example of this variation. A facility-level survey covering three of the county's seven sub-counties identified six different electronic medical record platforms in use (OpenMRS, KenyaEMR, IQCare, E-Hospital, Funsoft, and SYHOS), and several of the sampled facilities operated more than one system for managing patients (Juma et al., 2020). Most sampled sites in Kisumu Central ran two such systems, and one sampled facility in Muhoroni used both IQCare and SYHOS. A blockchain interoperability layer built on top of this environment would have to reconcile this platform heterogeneity rather than assume it away, which is exactly the inheritance problem the DeLone and McLean lens anticipates.

Seen through the DeLone and McLean lens, a blockchain interoperability layer placed above such a heterogeneous set of source systems will inherit their quality deficiencies rather than correct them. Logically, this dimension comes before the technical and organisational dimensions, because both depend on source systems producing good-quality data before they can function.

Applying the technical dimension

The technical dimension combines the Blockchain Trilemma and Parkerian Hexad.

Kenya's variation in connectivity, electricity, computing infrastructure, and health-information-system maturity across counties creates technical constraints for any national blockchain architecture. The Blockchain Trilemma suggests that architectural choices

must explicitly balance decentralisation, security, and scalability.

In such a setting, a permissioned or consortium-based architecture may be more compatible with the governance and performance requirements of a national health system than a fully open and decentralised blockchain. Such an architecture could permit authorised national and county actors to participate under defined governance arrangements while limiting the computational and governance burdens associated with unrestricted decentralisation.

The Parkerian Hexad provides a complementary mechanism for assessing whether the selected architecture preserves confidentiality, integrity, availability, possession or control, authenticity, and utility.

Kenya's Data Protection Act and digital-health regulatory framework establish legal obligations relevant to several of these properties. However, not every security property is necessarily addressed through an equivalent statutory requirement. Availability and utility, for example, require substantial engineering and operational attention. The framework therefore distinguishes between legal compliance and technical assurance, rather than assuming that compliance automatically establishes technical readiness

Applying the organisational dimension

The organisational dimension, combining Institutional Theory and Resource Dependence Theory, addresses how counties will behave under the legitimacy and resource pressures the devolved governance structure creates. Counties are structurally dependent on national equitable-share transfers under Article 202 of the Constitution and Article 203's revenue-sharing formula, and on donor co-financing that flows in part through national mechanisms and in part directly to county programmes. Both national and donor resource controllers require documentary evidence of readiness, compliance, and capacity as conditions for continued funding.

Institutional theory predicts that where documentation is produced primarily to satisfy such external legitimacy pressures, formal readiness artefacts may decouple from operational capacity, particularly for counties facing the greatest legitimacy pressure. Resource dependence theory identifies national line ministries and major donor programmes as the specific external actors whose documentary expectations shape county-level artefact production. Together, the two lenses predict that documentation-based readiness assessments should be interpreted as measures partly of legitimacy signalling and partly of operational capacity, with the mix varying by county and by the pressure environment specific counties face. This is a diagnostic prediction the framework makes rather than a claim about any particular county; it identifies where documentation and execution should be independently verified rather than assumed to co-vary.

Kisumu County again offers a concrete illustration of the organisational dimension in operation. When the Ministry of Health selected a pilot site for the national Electronic Community Health Information System in 2021, Kisumu was among the counties selected early partly because it already possessed the infrastructure that made it more efficient to build on existing capacity, with implementing partners playing a documented role in the county's scale-up (Ileri et al., 2025). That selection pattern is consistent with the kind of organisational behaviour institutional theory and resource dependence theory predict: national and donor actors used observed county capacity, not merely stated intent, to allocate a resource, in this case, the pilot itself. The same dynamic that made Kisumu an early adopter for community health digitisation would be expected to shape which counties are treated as ready for a blockchain interoperability pilot.

Cross-dimensional diagnostic reading

When the three dimensions are considered together, the framework identifies a specific configuration of readiness constraints in the

Kenyan devolved health governance context: a legally mandated national interoperability architecture (CIHIS) whose successful deployment depends simultaneously on source-system quality that varies across counties (systemic), on architectural choices that must accommodate infrastructure heterogeneity while preserving statutorily-required security properties (technical), and on organisational reporting practices whose alignment with operational reality is a function of legitimacy and resource pressures (organisational).

The contribution of the framework is therefore not to predict which dimension will necessarily be most restrictive in a particular county. Rather, it specifies which class of evidence should be examined to answer each readiness question.

For Kisumu, for example, evidence of organisational capacity associated with early digital-health implementation exists alongside evidence of source-system fragmentation. Neither observation alone establishes readiness for blockchain interoperability. Their combination illustrates precisely why an undifferentiated readiness score could obscure important differences across dimensions

Benchmarking against an existing readiness framework

The WHO-ITU National eHealth Strategy Toolkit (World Health Organization & International Telecommunication Union, 2012) is the most widely referenced international instrument for assessing and developing national eHealth strategies, and recent continental assessments continue to use it as the benchmark against which African national strategies are scored (Olufadewa et al., 2024). The toolkit and the present framework share a starting premise – that readiness is multi-component rather than a single score – but differ in unit of analysis and in what each treats as the binding constraint. The toolkit assesses a national strategy document against components such as vision and strategy, an implementation

plan, a monitoring and evaluation component, and adherence to data-standard principles; its unit of analysis is the policy document itself, and a country scores well when its strategy addresses each component on paper. The integrated framework proposed here instead treats technical capacity, organisational legitimacy, and source-system quality as properties of the health system that a strategy document describes, rather than as properties of the document, and it explicitly predicts, through institutional theory's decoupling mechanism, that a strategy document can score well on the toolkit's criteria while the underlying system remains unready on one or more of the three dimensions identified here. Applied to Kisumu, the two instruments would likely diverge: Kenya's national eHealth policy documents score reasonably well on toolkit-style criteria, having a stated vision, an implementation plan, and monitoring provisions, yet the county-level evidence reviewed above shows systemic fragmentation that the toolkit's document-level criteria would not detect. The integrated framework's comparative contribution is therefore to supply a system-level, not merely a document-level, diagnostic that can be layered onto strategy-assessment tools such as the toolkit rather than replacing them.

A second comparison is useful because the WHO-ITU toolkit is a strategy-assessment instrument rather than an empirical readiness model applied through fieldwork. Balasubramanian et al. (2021) developed a stakeholder-based blockchain readiness framework spanning motivational, engagement, technological, and structural dimensions, and tested it empirically through a multi-method case study combining a systematic literature review with stakeholder-level assessment in the United Arab Emirates healthcare sector. That framework and the one proposed here share an ambition to move beyond a single readiness lens, and both treat organisational and structural conditions as central rather than incidental. They differ in two respects relevant to the

present argument. First, Balasubramanian et al.'s framework is built around the readiness of individual stakeholder groups, government, providers, technology vendors, and patients, within a single national health system, whereas the framework proposed here is built around a devolved governance structure in which national and county levels can display different degrees of readiness on the same dimension. Second, their framework does not incorporate an explicit mechanism for anticipating when stated or documented stakeholder readiness might diverge from operational capacity; the present framework, through institutional theory's concept of decoupling, treats that divergence as a central diagnostic question rather than an incidental finding. The comparison also exposes a genuine asymmetry the present paper does not obscure: Balasubramanian et al.'s framework has been tested empirically against primary stakeholder data, whereas the framework proposed here remains a conceptual proposition pending the validation exercise described in the preceding limitations.

Limitations of the proposed framework

Three limitations qualify the framework's diagnostic claims. First, organising readiness into three dimensions is itself a simplification: the boundaries between technical, organisational, and systemic constraints are analytically useful but not always empirically crisp – a facility's poor data quality, for example, may itself be a downstream consequence of organisational under-investment rather than a purely independent systemic condition. Second, the framework treats the three dimensions as capable of moving independently for diagnostic purposes, but it does not claim they are statistically or causally independent; cross-dimensional interactions, for instance whether organisational legitimacy pressure shapes which systemic data-quality problems get reported at all, are plausible and are not modelled here. Third, because the framework has not undergone expert or empirical validation, its

assignment of specific lenses to specific dimensions, while argued from each lens's original theoretical claim, remains a proposition rather than a demonstrated allocation; a future Delphi exercise could reveal that practitioners assign some of these constructs differently than the paper does.

4.0 Conclusion

This paper has integrated five theoretical lenses spanning technical, organisational, and systemic dimensions into a single conceptual framework for blockchain health interoperability readiness in LMIC settings. The framework's contribution is diagnostic rather than predictive: it offers a structured basis for identifying which dimension of readiness is binding in a given context, rather than treating technical, organisational, and systemic constraints as an undifferentiated readiness problem. Kenya's devolved health system illustrates the framework's application without requiring primary data; companion empirical work by the author reports the corresponding evidence (Halwenge, 2026). The integration is not merely additive: it specifies both the division of theoretical labour between lenses sharing a dimension and the resolution of tensions between lenses operating across dimensions. Future work might extend the framework to settings with different devolution architectures, or test whether the three dimensions are jointly exhaustive or a fourth such as financial sustainability is required.

5.0 Recommendations

The recommendations that follow translate the framework's diagnostic contribution into concrete guidance for the research community, for policymakers designing digital health governance in LMIC settings, and for practitioners commissioning blockchain-based interoperability solutions. Each recommendation identifies both the value the framework offers and the implications that follow from adopting it.

Value of the integrated framework

The primary value of the integrated framework is analytical clarity. By assigning each lens to a distinct readiness dimension, the framework enables researchers and policymakers to identify, in advance of empirical inquiry, which dimension a given readiness question actually concerns preventing both the aggregation error and the attribution error. A secondary value is the sequencing implication that the systemic dimension is logically prior to the other two: readiness assessments that skip source-system quality are likely to misattribute the resulting variance to technical or organisational causes.

Operationalising this value requires translating the framework into an assessment instrument rather than leaving it as a conceptual map. A practical version would take the form of a scored checklist with three sub-scores, one per dimension, each built from a small number of directly observable or documentary indicators: for the technical dimension, architecture type and evidence of Parkerian Hexad property coverage in a security audit; for the organisational dimension, an independent verification step comparing documented compliance artefacts against a sample of operational records; and for the systemic dimension, a count of distinct source-system platforms in concurrent use and an assessment of their data-quality conformance, along the lines of the platform-fragmentation evidence reported for Kisumu County above. Unlike a single composite readiness score, the three sub-scores would be reported and acted on separately, since the framework's central claim is that a high score on one dimension does not offset a low score on another.

Implications for researchers

First, single-lens studies should be explicit about which dimension of readiness they address and should avoid extrapolating findings on one dimension (for example, technical security capacity) into claims about another (for example, organisational readiness), since the

integrated framework predicts these dimensions can move independently.

Second, readiness assessment instruments that rely on documentary or self-reported evidence should anticipate, rather than be surprised by, divergence between documented and operational indicators wherever institutional theory's decoupling mechanism is plausible that is, wherever the assessed organisation faces legitimacy or resource pressure from an external evaluator. Instrument design should build in independent verification of operational indicators rather than treating documentation as a sufficient proxy.

Third, the systemic dimension should be treated as logically prior in study design: where source-system quality has not been established, studies of technical or organisational readiness risk attributing to those dimensions variance that is properly explained by upstream data quality. Sequencing study designs establishing systemic quality before assessing technical and organisational readiness will generally produce cleaner causal inference than treating all three dimensions as simultaneous, independent predictors.

Implications for policymakers and practitioners

For policymakers responsible for national digital health architecture in devolved systems, the framework recommends that certification and readiness regimes be structured to test all three dimensions separately, rather than allowing high performance on documentary indicators to substitute for evidence of operational and source-system capacity. For practitioners commissioning blockchain-based interoperability solutions in LMIC contexts, the framework recommends that architectural choices, for example, permissioned versus fully decentralised ledgers be justified explicitly against both the technical dimension (trilemma trade-offs and hexad security properties) and the systemic dimension (source-system quality

inheritance), rather than on technical grounds alone.

Concretely, this could take the form of: requiring counties to report technical, organisational, and systemic sub-scores separately in annual digital-health readiness returns to the Digital Health Agency, rather than a single composite figure; commissioning independent, sampled verification of a subset of documentary compliance claims each reporting cycle, rather than accepting self-reported documentation at face value; and publishing county-level source-system inventories, of the kind compiled for Kisumu in this paper, as a standing input to national interoperability planning under the Digital Health Act (2023).

References

- Balasubramanian, S., Shukla, V., Sethi, J. S., Islam, N., & Saloum, R. (2021). A readiness assessment framework for Blockchain adoption: A healthcare case study. *Technological Forecasting and Social Change*, 165, 120536. <https://doi.org/10.1016/j.techfore.2020.120536>
- Chimbo, B., & Motsi, L. (2024). The effects of electronic health records on medical error reduction: Extension of the DeLone and McLean information system success model. *JMIR Medical Informatics*, 12, e54572. <https://doi.org/10.2196/54572>
- Constitution of Kenya. (2010). *National Council for Law Reporting*. <http://www.kenyalaw.org/kl/index.php?id=398>
- Data Protection Act, No. 24 of 2019 (Kenya). http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf
- 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>
- Digital Health Act, No. 15 of 2023 (Kenya). http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2023/TheDigitalHealthAct_No.15of2023.pdf
- Digital Health (Health Information Management Procedures) Regulations, 2025 (Kenya). <https://new.kenyalaw.org/akn/ke/act/ln/2025/76/eng@2025-04-11>
- 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. <https://doi.org/10.2307/2095101>
- Halwenge, P. M. (2026). *A blockchain-based interoperability framework for Kenya's integrated health records* [Unpublished doctoral dissertation]. Technical University of Kenya.
- Health Act, No. 21 of 2017 (Kenya). <https://new.kenyalaw.org/akn/ke/act/2017/21/eng@2022-12-31/source>

Directions for future research

Two lines of future work would strengthen the framework. First, empirical testing across multiple LMIC settings would clarify whether the three dimensions identified here are jointly exhaustive of readiness variance or whether a fourth dimension such as financial sustainability or workforce continuity should be added. Second, comparative application of the framework across devolved health systems with different constitutional configurations would clarify the extent to which the diagnostic categories generalise beyond the Kenyan case used illustratively here.

- Ileri, S., Waiganjo, P., Ochieng, D. O., Kagiri, M., Anindo, M., Adoyo, M., Wanjiru, R., Kirui, J., Pundo, R., Kimani, M., & Wanyungu, J. (2025). An exploration of the successful scale-up of the electronic community health information system in Kenya. *Oxford Open Digital Health*, 3, oqaf020. <https://doi.org/10.1093/oodh/oqaf020>
- Isemeck, C. S., Nguni, K., Kariuki, J., & Muchene, O. (2019). Factors influencing the adoption of electronic health records in public health facilities in Kisumu County, Kenya. *Journal of Health, Medicine and Nursing*, 4(1), 74–101. <https://iprjb.org/journals/JHMN/article/view/826>
- Joshi, S., & Sharma, M. (2023). Assessment of implementation barriers of blockchain technology in public healthcare: Evidences from developing countries. *Health Systems*, 12(2), 223–242. <https://doi.org/10.1080/20476965.2023.2206446>
- Juma, R., Abila, J., & Oluoch, J. (2020). Electronic medical records software types in use within Kisumu County. *International Journal of Innovative Science and Research Technology*, 5(5), 1989–1992. <https://doi.org/10.38124/ijisrt20may395>
- Kenya Ministry of Health. (2016). *National eHealth policy 2016–2030*. Government of Kenya. <https://www.health.go.ke/wp-content/uploads/2016/04/Kenya-National-ehealth-Policy-final-1.pdf>
- Kenya Ministry of Health. (2020). *Kenya health information systems interoperability framework*. Government of Kenya. https://www.data4sdgs.org/sites/default/files/services_files/Kenya%20Health%20Information%20Systems%20Interoperability%20Framework.pdf
- Kore, T., Rorissa, A., & Mamo, G. (2026). Healthcare institutions readiness towards blockchain technology adoption: A case study of hospitals in Ethiopia. *Discover Health Systems*, 5, 34. <https://doi.org/10.1007/s44250-026-00367-2>
- Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340–363. <https://doi.org/10.1086/226550>
- Olufadewa, I. I., Iyiola, O. P., Nnatus, J., Fatola, K., Oladele, R., Olufadewa, T., Adesina, M., & Udofia, J. (2024). National eHealth strategy frameworks in Africa: A comprehensive assessment using the WHO-ITU eHealth strategy toolkit and FAIR guidelines. *Oxford Open Digital Health*, 2, oqae047. <https://doi.org/10.1093/oodh/oqae047>
- Parker, D. B. (2014). Toward a new framework for information security. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer security handbook* (6th ed., pp. 3.1–3.23). Wiley. <https://doi.org/10.1002/9781118820650.ch3>
- Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence perspective*. Harper & Row.
- World Health Organization & International Telecommunication Union. (2012). *National eHealth strategy toolkit*. International Telecommunication Union. <https://apps.who.int/iris/handle/10665/75211>
- Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. *IEEE Access*, 8, 16440–16455. <https://doi.org/10.1109/ACCESS.2020.2967218>