Blockchain-Enabled Governance of Enterprise Data Asset Recognition in Information Systems: Risks, Mechanisms, and Strategic Policy Paths

Haoran Li[1], Selma Kovacevic[2, *]
[1]School of Information Management, Anhui Xinhua University, Hefei, China, 230088
[2] Faculty of Economics, University of Zenica, Zenica, Bosnia and Herzegovina, 72000
[*]Email: selma.kovacevic@unze.edu.ba (Corresponding Author)

Abstract

This study examines how blockchain can strengthen the recognition, valuation, disclosure, and supervision of enterprise data assets in information systems. It develops a multi-actor governance framework involving firms, auditors, platform operators, and regulators, and analyzes how blockchain capabilities reconfigure incentives, verification routines, and accountability structures across the data-asset life cycle. Building on the literature on blockchain, accounting information systems, digital reporting, auditing, and supply-chain traceability, the paper identifies four recurring governance failures: asset inflation, verification collusion, data leakage, and fragmented oversight. It then explains how shared ledgers, smart contracts, permissioned access, and auditable process logs can reduce these failures, while also introducing new organizational and regulatory tensions. The paper proposes a staged policy path that combines technical design, institutional rules, audit redesign, and incentive alignment. The contribution lies in connecting enterprise information systems research with the emerging problem of data-asset recognition, and in offering a structured governance logic for organizations and regulators seeking credible digital accounting infrastructures.

Keywords: data asset recognition; blockchain governance; accounting information systems; audit transparency; enterprise information systems

Article History:
Received February 20, 2025
Revised April 24, 2025
Accepted June 20, 2025
Available Online June 30, 2025

Blockchain-Enabled Governance of Enterprise Data Asset Recognition in Information Systems: Risks, Mechanisms, and Strategic Policy Paths

1. Introduction

Data has become a strategic production factor in contemporary organizations, yet enterprise information systems still struggle to treat data assets as economically meaningful, verifiable, and governable resources. Digital platforms, cloud-based infrastructures, algorithmic services, and connected devices continuously generate records that shape operational decisions, pricing, customer interactions, and innovation trajectories. Even so, the accounting and governance treatment of these resources remains uneven. Firms may own, control, license, exchange, enrich, or repeatedly reuse data, but they often lack stable methods for deciding when a dataset becomes an identifiable asset, how that asset should be measured, how value creation should be documented, and how disclosures should be verified. This mismatch between economic reality and reporting practice has made data-asset recognition one of the most difficult frontiers in digital accounting and enterprise information systems research.

The problem is not only technical. It is also organizational, institutional, and behavioral. In most firms, data assets are created through a long chain of processes involving information acquisition, integration, cleaning, model training, customer interaction, process monitoring, and downstream commercial use. Each stage can alter quality, rights, provenance, and value. Traditional accounting information systems were designed for relatively stable transactions and well-bounded tangible or contractual assets; they were not designed for fast-moving, multi-source, reconfigurable data objects whose value depends on context, reuse, and interoperability. As a result, the recognition of data assets often suffers from uncertain ownership, weak audit trails, inconsistent valuation assumptions, and poor cross-functional accountability. These weaknesses open space for opportunistic reporting, selective disclosure, duplicated capitalization, and governance failure.

Recent studies in blockchain and information systems suggest that distributed ledger technologies may offer a credible infrastructure for recording, validating, and governing data-intensive processes. Foundational research framed blockchain as a shared, tamper-resistant record-keeping mechanism with implications for transactions, trust, and distributed coordination (Pilkington, 2016; Yuan & Wang, 2018; Yli-Huumo et al., 2016). Later work translated these capabilities into enterprise information systems, emphasizing operating mechanisms, implementation logic, and integration pathways across industries (Lu, 2018a, 2018b, 2019, 2022; Zheng & Lu, 2022; Lei & Ngai, 2023; Lacity, 2022). In parallel, studies on Industry 4.0, IoT security, logistics, healthcare information management, and accounting information systems show that blockchain can improve traceability, reduce reconciliation costs, and support auditable data flows (Da Xu et al., 2021; Chen et al., 2024; Huo et al., 2022; Prybutok et al., 2022; Adere, 2022).

Accounting literature has become increasingly attentive to these possibilities. Researchers argue that blockchain may reshape bookkeeping, auditability, internal controls, and continuous assurance by enabling shared ledgers, smart contracts, and near real-time

ISSN: 3068-7462 https://doi.org/10.63646/jeagf.2025.030201

verification (Dai & Vasarhelyi, 2017; Coyne & McMickle, 2017; Schmitz & Leoni, 2019; Bonson & Bednarova, 2019; Han et al., 2023). More recent studies examine blockchain adoption in accounting, the integration of blockchain with ERP, IoT, and XBRL, and the organizational constraints that prevent these systems from moving beyond conceptual enthusiasm (Fullana & Ruiz, 2021; Faccia & Petratos, 2021; Akter et al., 2024; Nofel et al., 2024; Sunmola & Lawrence, 2024). Yet a central question remains insufficiently answered: how can blockchain be translated into a governance architecture for recognizing and supervising enterprise data assets rather than merely documenting transactions?

That question matters because data-asset recognition is more exposed to manipulation than many conventional reporting items. Data are replicable, combinable, and easy to alter without visible physical traces. The same dataset can be used in multiple business processes, embedded in analytics pipelines, and repeatedly refined through machine learning or human annotation. Rights may be fragmented across creators, processors, users, and platforms. Value may depend on downstream utility, exclusivity, privacy constraints, and complementary capabilities. This means that the recognition of a data asset is never purely bookkeeping exercise. It is an organizational claim about provenance, control, future benefits, compliance, and the credibility of internal evidence. If that claim is weak, the firm's digital reporting infrastructure becomes vulnerable to asset inflation, verification collusion, selective omission, and regulatory disputes.

Blockchain is relevant here not because it automatically solves valuation uncertainty, but because it can restructure the evidentiary environment in which recognition decisions are made. Shared ledgers can preserve process history; smart contracts can encode recognition rules and approval sequences; permissioned networks can distribute access while protecting confidentiality; and immutable logs can strengthen ex post accountability. These features align well with the control needs of data governance, but they also introduce trade-offs involving integration cost, scalability, privacy design, legal enforceability, and the distribution of authority across firms, auditors, platform operators, and regulators. The effectiveness of blockchain therefore depends on governance design, not only on technical deployment.

This paper addresses the issue by developing a conceptual article whose logic parallels the uploaded manuscript but shifts the emphasis from a narrow incentive-penalty model toward a broader enterprise information systems perspective. Rather than reproducing the original article's formal game equations, the present study reconstructs the same analytical sequence: it first identifies the risks embedded in data-asset recognition, then explains how blockchain can empower regulation and control, next build a multi-actor governance framework, and finally derives strategic policy paths for implementation. In doing so, it integrates the user-specified scholarship by Lu and colleagues with adjacent work in accounting, supply chains, ERP integration, IoT, and digital reporting.

The paper makes three contributions. First, it extends the blockchain-information-systems literature by focusing on data-asset recognition as a governance problem rather than a purely technical or accounting problem. Second, it contributes to blockchain-accounting research by connecting auditability and shared-ledger concepts to the distinctive

ISSN: 3068-7462 https://doi.org/10.63646/jeagf.2025.030201

characteristics of enterprise data assets, including replicability, contextual valuation, and rights fragmentation. Third, it provides a strategic policy framework for organizations and regulators, showing that credible recognition requires coordinated change across technology design, internal controls, audit procedures, and institutional incentives. The remainder of the paper is organized as follows. Section 2 reviews the relevant literature. Section 3 analyzes the enterprise workflow and blockchain-enabled governance mechanism. Section 4 develops the analytical framework. Section 5 examines governance scenarios and policy paths. Section 6 discusses theoretical and practical implications, and Section 7 concludes.

2. Literature Review

2.1 Blockchain in Enterprise Information Systems

Early blockchain research concentrated on architecture, consensus, security, and emerging application domains. Systematic reviews established the field's foundational vocabulary, distinguishing decentralization, persistence, auditability, and programmable transactions as the core properties of distributed ledgers (Conoscenti et al., 2016; Yli-Huumo et al., 2016; Casino et al., 2019). Dinh et al. (2018) recast blockchain as a data-processing infrastructure rather than merely a cryptocurrency engine, while Lu's series of review papers synthesized functions, applications, research issues, and implementation patterns from an information systems perspective (Lu, 2018a, 2018b, 2019, 2022). Zheng and Lu (2022) showed that blockchain research in information systems had moved from technological curiosity toward platform ecosystems, governance, and implementation logic. Lei and Ngai (2023) further documented that blockchain studies in information systems increasingly rely on adoption theories such as TAM, TOE, and diffusion perspectives, yet often under-specify the technical artifact itself. Collectively, these studies indicate that blockchain is not valuable in isolation; its organizational effects depend on how it is embedded in enterprise processes, governance routines, and inter-organizational relationships.

A second stream examines integration with adjacent enterprise technologies. Research on ERP, Industry 4.0, supply chains, and IoT shows that blockchain can complement existing systems by improving traceability, inter-firm coordination, and process automation rather than by replacing enterprise architectures outright. Dasaklis et al. (2021), Haddara et al. (2021), Faccia and Petratos (2021), Kitsantas et al. (2022), and Sunmola and Lawrence (2024) each argue that ERP-blockchain integration is most beneficial when firms face multi-party data reconciliation problems, fragmented documentation, and trust-sensitive workflows. Chen et al. (2024) and Da Xu et al. (2021) extend the argument to Industry 4.0 and IoT security, where blockchain strengthens the integrity of machine-generated data and helps coordinate heterogeneous digital actors. These studies are especially relevant for data-asset recognition because most enterprise data assets are not created in stand-alone accounting systems; they emerge from ERP, IoT, platform, and analytics environments that already span multiple organizational boundaries.

The supply-chain and logistics literature adds another important insight: blockchain adoption succeeds when organizations face problems of provenance, transparency, and shared accountability. Kshetri (2018), Treiblmaier (2018), Wang et al. (2019), Saberi et al. (2019), Gurtu and Johny (2019), Wamba and Queiroz (2020), Wong et al. (2020), Wamba et al. (2020), Tandon et al. (2021), Upadhyay et al. (2021), Ali et al. (2021), Benzidia et al. (2021), Saurabh and Dey (2021), Sahebi et al. (2022), and Sahoo et al. (2024) show that blockchain performs best in settings where multiple actors need synchronized records but do not fully trust one another. This directly parallels the data-asset setting, in which firms, auditors, data providers, regulators, and users require common evidence about data provenance and authorized use. The literature therefore suggests that data-asset recognition should be analyzed as a coordinated governance problem involving shared records, not as an internal bookkeeping choice alone.

2.2 Blockchain and Accounting Information Systems

Accounting scholarship has explored blockchain through the lenses of bookkeeping redesign, auditability, reporting quality, and the future role of accountants. Dai and Vasarhelyi (2017) and Coyne and McMickle (2017) provided early arguments that blockchain could support triple-entry logic, shared ledgers, and higher assurance in transaction recording. Schmitz and Leoni (2019) emphasized the need for a research agenda linking blockchain to organizational control and the changing role of audit. Bonson and Bednarova (2019) highlighted implications for transparency and professional judgment. Liu et al. (2019) differentiated permissionless and permissioned architectures for accounting and auditing, while Han et al. (2023) later synthesized these debates into four themes: event-based accounting, real-time accounting, triple-entry bookkeeping, and continuous auditing. Taken together, these studies establish that blockchain may improve accounting information quality, but they also warn that institutional change and professional adaptation are necessary for implementation (Table 1).

Table 1. Research streams and unresolved gaps

Stream	Representative focus	Main insight	Gap addressed in this article
Blockchain foundations	Consensus, immutability, smart contracts, distributed trust	Explains why ledgers reduce reconciliation and tampering risk	Rarely links technical affordances to data-asset recognition workflow
Accounting and auditing	Triple-entry accounting, audit automation, assurance logic	Shows that blockchain can reshape evidence and audit timing	Limited treatment of data assets as the object of recognition
Enterprise systems	ERP integration, shared records, interoperability	Highlights process integration and cross-functional coordination	Underexplores governance incentives among firms, auditors, and regulators
Supply chain / IoT / healthcare	Traceability, data sharing, privacy, ecosystem trust	Demonstrates blockchain value in multi-party data environments	Application insights are seldom translated into accounting governance mechanisms

ISSN: 3068-7462 https://doi.org/10.63646/jeagf.2025.030201

Subsequent studies broadened the accounting information systems perspective. Huerta and Jensen (2017) linked AIS research to data analytics and big data, thereby offering a bridge between conventional reporting systems and data-intensive organizational environments. Wu et al. (2019) proposed that the combination of IoT and blockchain can improve accounting information quality by strengthening the capture and verification of operational events. Demirkan et al. (2020) discussed cybersecurity, governance, and accounting implications. Fullana and Ruiz (2021) argued that the blockchain era forces AIS research to re-evaluate system boundaries, control assumptions, and the relationship between firms and regulators. Faccia and Petratos (2021) examined blockchain, ERP, and AIS integration through the case of e-procurement and system integration, while Nofel et al. (2024) expanded the discussion by combining blockchain with IoT and XBRL in digital reporting architectures. Akter et al. (2024) added empirical evidence that blockchain accounting adoption is shaped by organization-specific barriers such as integration complexity, knowledge gaps, and implementation cost. This stream shows strong conceptual momentum but still lacks a mature framework for governing data-asset recognition specifically.

2.3 Data Assets, Digital Reporting, and Audit Governance

More recent literature focuses on data-rich reporting environments and the governance challenges associated with digital assets, information sharing, and audit quality. Prybutok et al. (2022) and Adere (2022) demonstrate that blockchain can manage sensitive information and identity-rich records when trust and traceability matter. Mamun et al. (2022) show similar potential in electronic health records management. Giang et al. (2023), Abdullah and Almaqtari (2024), and Jiang et al. (2024) argue that blockchain may strengthen business accounting through enhanced transparency, real-time information sharing, and data integrity, though benefits depend on integration design and managerial capability. Qader et al. (2024) suggest that blockchain and artificial intelligence together may improve audit quality, but only when underlying data are structured, verified, and governed consistently. These studies do not directly solve data-asset recognition, yet they demonstrate that digital reporting credibility depends on the architecture through which records are created, shared, and audited.

The audit-governance literature also underscores a persistent tension between transparency and discretion. Permissioned ledgers can increase the verifiability of controls, but they may also redistribute responsibility among system designers, external auditors, and regulatory institutions. In practice, auditable records do not eliminate judgment; they move judgment to earlier stages of design, configuration, and access control. This is especially important for data assets because value depends on context, rights, and future use. A blockchain record may show who created or modified a dataset, but it does not by itself determine whether the dataset satisfies recognition criteria, whether valuation assumptions are reasonable, or whether legal restrictions undermine future economic benefit. Audit governance in this domain therefore requires a combination of immutable process evidence and domain-specific professional interpretation.

2.4 Literature Gaps

The literature reviewed above reveals four gaps. First, blockchain research in information systems is rich in application mapping but comparatively weak in explaining how blockchain changes the recognition and control of data-intensive intangible assets inside the firm. Second, accounting studies focus heavily on transaction recording and continuous assurance, whereas data-asset recognition involves upstream issues of provenance, quality, rights, exclusivity, and reuse. Third, studies of blockchain adoption in ERP, supply chains, and IoT highlight organizational coordination, yet they seldom connect those insights to the reporting and supervision of recognized data assets. Fourth, audit research acknowledges the role of shared ledgers but rarely specifies how firms, auditors, regulators, and platform operators should divide responsibilities when asset recognition depends on digitally generated evidence. This paper addresses these gaps by treating enterprise data-asset recognition as a multi-actor governance process supported—but not fully determined—by blockchain-enabled information systems.

3. Enterprise Data-Asset Recognition Workflow and Blockchain-Enabled Governance Mechanism

3.1 The Workflow of Enterprise Data-Asset Recognition

In practice, enterprise data-asset recognition unfolds through a sequence of interdependent stages rather than a single accounting event. The first stage is origination and rights clarification. Here, firms identify datasets produced internally or acquired externally, define usage rights, and document restrictions related to privacy, licensing, confidentiality, and third-party dependence. The second stage is data qualification, in which datasets are cleaned, standardized, linked to metadata, and assessed for relevance, reliability, completeness, and lawful processability. The third stage is value articulation. Managers determine whether the dataset is expected to generate future economic benefit directly through sale or licensing, or indirectly through analytics, service improvement, risk reduction, or model training. The fourth stage is recognition and reporting, where accounting teams decide whether the asset should be disclosed, how it should be classified, and what supporting documentation is required. The fifth stage is post-recognition monitoring, involving impairment review, access control, usage tracking, and assurance over continuing compliance. Each stage depends on information produced by different units, which means that evidence quality can deteriorate when process integration is weak.

This workflow exposes several governance bottlenecks. Rights may be ambiguous when datasets are co-created with customers, platform partners, or outsourced processors. Quality assessments may be inconsistent when data pass through multiple transformation pipelines. Economic benefit claims may be overstated when managers rely on speculative scenarios or when a dataset's usefulness depends on complementary assets that the firm does not yet control. Recognition decisions may also be distorted by managerial incentives, especially when capitalization improves financing narratives or innovation signaling. Finally, post-recognition monitoring may be neglected because many firms treat data assets as static reporting objects even though their quality, legality, and strategic value change

ISSN: 3068-7462 https://doi.org/10.63646/jeagf.2025.030201

continuously. These bottlenecks explain why data-asset recognition requires an infrastructure for evidence continuity rather than one-off documentation.

3.2 Four Recurring Governance Failures

The first failure is asset inflation. Managers may overstate the uniqueness, readiness, or economic usefulness of a dataset, especially when competitive pressure or capital-market expectations reward digital transformation narratives. Inflation can occur through aggressive inclusion of low-quality records, repeated capitalization of overlapping datasets, vague assumptions about monetization, or a failure to separate raw data from value-creating processing capabilities. The second failure is verification collusion. When external assurance providers lack granular traceability or depend heavily on management-provided documentation, audit routines may drift toward form over substance. Auditors may accept incomplete provenance records, unverifiable processing logs, or narrow samples that do not capture the actual governance history of the asset.

The third failure is data leakage and unauthorized reuse (Table 2). Recognition often requires wider visibility over datasets, access controls, transformation history, and usage records. If these processes are not governed carefully, the very act of documenting and verifying data assets can increase exposure to cyber risk, internal misuse, and contractual breach. The fourth failure is fragmented oversight. Data governance teams, accounting functions, compliance officers, cybersecurity staff, external auditors, and regulators typically rely on different systems and reporting formats. Fragmentation produces information silos and weakens accountability because no single record links origination, processing, valuation, approval, and later use. These failures are not isolated; they reinforce one another. Weak provenance makes asset inflation harder to detect, fragmented oversight reduces the probability of identifying leakage or collusion, and poor post-recognition monitoring allows misstatements to persist over time.

Table 2. Risks across the recognition process and blockchain control levers

Recognition stage	Governance risk	Why the risk emerges	Blockchain-enabled control lever
Ownership clarification	Ambiguous rights and duplicated claims	Data may be generated jointly, copied easily, or licensed across units	Timestamped provenance records and rights-linked metadata
Preparation and valuation	Selective assumptions and inflated valuation	Context-dependent value and weak audit trail permit managerial discretion	Immutable logs of data transformation, model inputs, and approval events
Disclosure and reporting	Selective disclosure and privacy leakage	Firms may hide uncertainty while exposing sensitive information	Permissioned access, encrypted sharing, and event-based disclosure control
External assurance	Auditor dependence and collusion	Client pressure and opaque evidence reduce audit independence	Shared evidence layer, automated exception

ISSN: 3068-7462 https://doi.org/10.63646/jeagf.2025.030201

Recognition stage	Governance risk	Why the risk emerges	Blockchain-enabled control lever
			flags, and review traceability
Regulatory oversight	Fragmented supervision and delayed intervention	Authorities often see only final reports rather than process evidence	Consortium access, synchronized reporting, and smart-rule enforcement

3.3 Why Blockchain Is a Plausible Governance Infrastructure

Blockchain aligns with these problems because it offers a way to preserve process history across organizational boundaries. Research on shared ledgers and distributed verification emphasizes four properties that are especially valuable in the data-asset context: immutability of recorded events, synchronized visibility across authorized parties, programmable execution through smart contracts, and fine-grained permission structures in consortium or private networks (Christidis & Devetsikiotis, 2016; Luu et al., 2016; Dinh et al., 2018; Lu, 2022). Together, these properties can transform how recognition evidence is created and consumed. Rather than relying on static documents assembled after the fact, firms can generate time-stamped records as data are acquired, transformed, approved, and used. Auditors and regulators can then test the continuity of those records instead of depending solely on ex post managerial explanations (Figure 1).

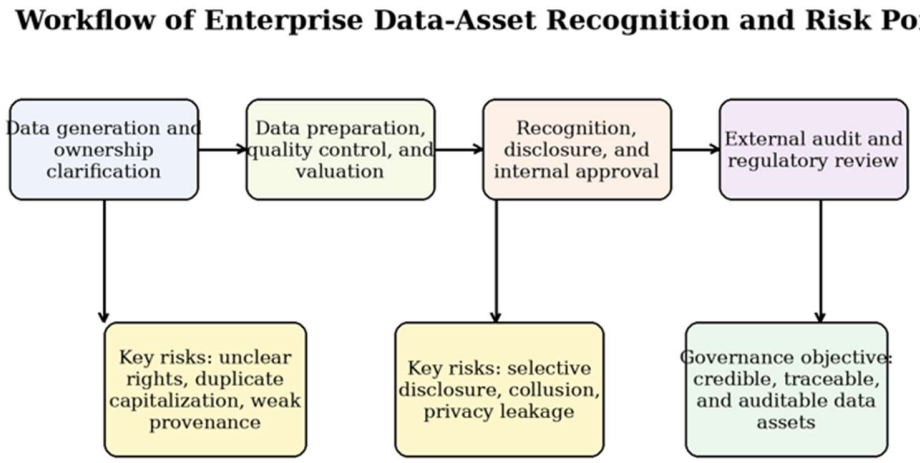

Figure 1. Workflow of enterprise data-asset recognition and risk points

A blockchain-enabled architecture for data-asset recognition does not require that all enterprise data be stored on-chain. In fact, full on-chain storage is usually undesirable because of volume, confidentiality, and performance constraints. A more credible architecture is hybrid. Core datasets remain off-chain in enterprise repositories, data lakes, or secure cloud environments, while key governance events are hashed, time-stamped, and recorded on a permissioned ledger. Such events may include data acquisition, rights

confirmation, quality certification, approval of transformation models, valuation review, access authorization, impairment triggers, and disposal decisions. This arrangement preserves privacy while still creating an immutable chain of governance evidence. It also allows different actors to verify that the reported process occurred in the claimed sequence without exposing all underlying commercial data.

3.4 Mechanisms of Blockchain-Enabled Governance

First, blockchain strengthens provenance. Each approved data-acquisition event can be linked to origin metadata, contractual rights, and responsible personnel. If later questions arise about legal basis or ownership, reviewers can trace the governance chain quickly. Second, blockchain improves process discipline. Smart contracts can enforce preconditions for recognition, such as completion of quality checks, legal review, or separation of duties between data custodians and financial approvers. Third, blockchain increases the cost of collusion. When approval steps, amendments, and exceptions are recorded across multiple authorized nodes, it becomes harder for a firm and an auditor to silently alter the evidence base. Fourth, blockchain supports continuous monitoring. Because post-recognition events such as access changes, model retraining, or rights expiration can also be logged, the asset remains governable after initial recognition rather than disappearing into static disclosure files.

Yet blockchain also has boundaries. Immutability can preserve poor-quality records just as easily as good ones if input controls are weak. Smart contracts can automate flawed rules if recognition criteria are badly designed. Permissioned governance can reduce transparency if access rights are overly concentrated. Integration costs can be substantial when firms rely on legacy ERP, fragmented metadata structures, or inconsistent master-data practices. Finally, the legal status of blockchain evidence may vary across jurisdictions. For these reasons, blockchain should be viewed as an accountability infrastructure that complements, rather than substitutes for, managerial judgment, audit competence, and regulatory standards (Figure 2).

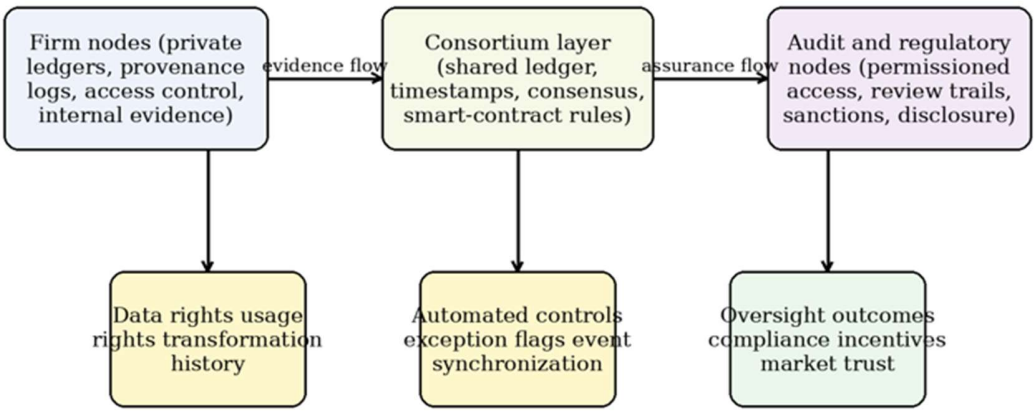

Figure 2. Blockchain-enabled governance architecture for data-asset recognition

3.5 A Governance Logic for Enterprise Information Systems

The central insight is that data-asset recognition becomes more credible when information systems shift from document-centric control to event-centric control. Traditional reporting practices often reconstruct asset histories retrospectively; blockchain-enabled systems can register decision-relevant events as they occur. This changes the balance of power in governance. Managers retain responsibility for economic interpretation, but they lose some discretion to retroactively reshape evidence. Auditors gain better access to process continuity, but they must expand their competence in system design, access protocols, and data lineage. Regulators can supervise through targeted access to standardized audit trails rather than through fragmented submissions alone. In this sense, blockchain does not merely increase transparency; it redistributes how transparency is generated, validated, and contested within enterprise information systems.

4. Analytical Framework: Actors, Governance Logic, and Research Propositions

4.1 Core Actors and Their Decision Logics

To mirror the governance logic of the source manuscript while avoiding textual imitation, this paper frames enterprise data-asset recognition as the interaction of four actors rather than three. The first actor is the focal firm, which wants to transform digital resources into recognized, useful, and strategically legitimate assets. The second actor is the assurance community, including external auditors, internal auditors, and specialized verification providers. The third actor is the platform layer, which includes ERP administrators, data-governance teams, cloud-service managers, and blockchain-network operators who configure the technical environment in which evidence is created. The fourth actor is the regulatory environment, including accounting standard setters, industry regulators, data-protection authorities, and supervisors who define disclosure expectations and enforcement intensity. This four-actor perspective is more suitable for enterprise information systems because technical architecture itself shapes organizational incentives.

Each actor faces a different optimization problem. Firms seek strategic flexibility, lower reporting costs, and favorable capital-market or stakeholder perceptions. Assurance providers seek credible evidence, manageable engagement risk, and procedural defensibility. Platform actors seek system stability, integration feasibility, cybersecurity resilience, and manageable governance complexity. Regulators seek comparability, credibility, enforceability, and reduced systemic reporting risk. These objectives overlap but do not perfectly align. Firms may prefer opacity when datasets are commercially sensitive. Auditors may prefer narrower scopes when system complexity is high. Platform actors may prioritize uptime over transparency if compliance routines are computationally costly. Regulators may require greater visibility than firms are willing to provide. Data-asset recognition therefore evolves inside a field of negotiated controls and incomplete alignment.

4.2 Governance Dimensions

ISSN: 3068-7462 https://doi.org/10.63646/jeagf.2025.030201

Building on the literature, the framework uses four governance dimensions. The first is evidentiary integrity: the degree to which provenance, transformation history, approvals, and post-recognition events are captured in a durable and testable way. The second is incentive alignment: the extent to which managerial, audit, and technical actors gain more from compliance than from opportunism, concealment, or weak control execution. The third is architectural interoperability: the extent to which ERP, data-lake, reporting, cybersecurity, and blockchain components exchange consistent metadata and authorization logic. The fourth is institutional legitimacy: the degree to which stakeholders believe the recognition process is fair, transparent, standards-consistent, and enforceable. A system can be technically advanced yet still fail if one of these dimensions is weak. For example, high integrity without interoperability may produce unusable evidence, while interoperability without incentive alignment may simply accelerate the spread of weak controls.

4.3 Recognition-Stage Logic

The framework assumes that credible recognition emerges when governance evidence accumulates progressively through the asset life cycle (Table 3). At origination, the emphasis is on rights and provenance. At qualification, the emphasis shifts to quality controls and metadata reliability. At value articulation, firms must demonstrate not only technical readiness but also a plausible pathway to future economic benefit and lawful use. At recognition, the key issue becomes whether approval rights and documentation standards were satisfied by independent roles. At post-recognition monitoring, the system must capture changes that affect continued validity, such as privacy restrictions, contract expiry, model drift, or impairment indicators. Blockchain can support all stages, but only if firms specify which events matter and what evidence each event must generate. In other words, blockchain does not define recognition criteria; it operates governance around those criteria.

Table 3. Actors, incentives, and governance instruments

Actor	Primary objective	Potential opportunism	Governance instrument
Firm	Recognize valuable data resources and signal digital capability	Inflated valuation, repeated capitalization, selective disclosure	Internal provenance controls, disclosure standards, rewards for compliant recognition
Auditor / assurer	Verify recognition and maintain professional legitimacy	Tolerance of weak evidence, collusion, overreliance on client representations	Permissioned evidence access, automated audit trails, penalties for collusion
Regulator	Preserve market credibility and enforce fair reporting	Delayed enforcement, uneven supervision, overreliance on ex post penalties	Consortium visibility, differentiated sanctions, interoperability standards
Technology platform	Record events and coordinate verification	False sense of assurance if rules are weak	Smart controls linked to explicit recognition criteria and review rights

4.4 Research Propositions

Proposition 1: The perceived credibility of recognized data assets increases when blockchain is used to record high-value governance events rather than raw data itself. The reason is that evidence continuity, not storage maximalism, is what strengthens assurance. Hybrid architecture reduces confidentiality and scalability problems while preserving traceability.

Proposition 2: Blockchain improves data-asset governance only when smart-contract rules are coupled with off-chain professional review. Fully automated approval is inappropriate because valuation and rights interpretation remain context dependent.

Proposition 3: The benefits of blockchain for data-asset recognition are strongest when the firm's information environment is already fragmented across multiple functions or partner organizations. In such settings, shared ledgers provide the greatest reduction in reconciliation cost and evidentiary ambiguity.

Proposition 4: Audit quality improves when permissioned blockchain access is granted at the process-event level rather than through static document packets, because auditors can examine the sequence, timing, and authorization history of recognition decisions.

Proposition 5: The risk of recognition inflation declines when post-recognition usage and impairment events are also logged on chain. This is because initial approval can be challenged by later evidence showing diminished utility, legal restrictions, or changing data quality.

Proposition 6: Regulatory legitimacy increases when blockchain-based reporting standards specify minimum metadata fields for provenance, rights, valuation assumptions, and lifecycle events. Without standardization, the same technology can produce incomparable evidence structures across firms.

Proposition 7: Platform actors become decisive governance intermediaries in blockchain-enabled recognition systems, because they configure the permissions, interfaces, and data-lineage models that determine what can later be audited. This implies that technical teams must be incorporated into accountability design rather than treated as neutral infrastructure providers.

Proposition 8: The governance value of blockchain is weakened when firms use it primarily as a symbolic signal of digital sophistication without redesigning internal controls, approval workflows, and assurance responsibilities.

4.5 Implications of the Framework

These propositions reposition enterprise information systems as the institutional backbone of data-asset recognition. In traditional settings, accountants and auditors mainly inspect outputs produced elsewhere. In the framework proposed here, the system itself becomes part of the governance object. Questions such as who approved a dataset, under what rights, following which transformation pipeline, and with what subsequent usage constraints become inseparable from the recognition decision. This has important theoretical implications. It suggests that data-asset recognition should be analyzed through socio-

technical governance rather than through accounting measurement alone. It also implies that blockchain is valuable not because it eliminates trust, but because it redistributes trust into traceable process design, coordinated permissions, and verifiable evidence. That distinction is crucial for avoiding technological determinism and for understanding why many blockchain experiments fail to generate real assurance benefits.

4.6 Boundary Conditions

The framework is most applicable in environments where data assets are strategically important, cross-functional, and repeatedly reused. It is less useful for small firms with simple data sets, low external disclosure needs, or minimal partner interdependence. It is also constrained where legal uncertainty is high, where data rights are deeply contested, or where confidentiality demands prohibit, meaningful evidence sharing even in permissioned form. Finally, the framework assumes some degree of digital maturity. Firms with poor master-data management, weak ERP integration, or unstable cybersecurity practices may need to address those fundamentals before blockchain produces meaningful governance gains. These boundary conditions do not negate the framework; they clarify when blockchain-enabled recognition is a realistic organizational choice and when it risks becoming a costly overlay on weak information systems.

5. Governance Scenarios and Strategic Policy Paths

5.1 Scenario One

High digital capability but weak recognition discipline. Some firms possess strong technical infrastructures yet weak reporting discipline. They generate large volumes of data, have mature analytics teams, and operate integrated platforms, but still lack clear rules for deciding when data become recognizable assets. In this scenario, blockchain should not be introduced as a broad symbolic innovation. Instead, it should be deployed selectively to enforce recognition gates. The most effective design is a permissioned workflow that records the completion of rights checks, data-quality certification, model documentation, valuation review, and independent approval. Smart contracts should require that no recognition entry is finalized before all governance checkpoints are satisfied. For these firms, the main benefit of blockchain is discipline through sequencing. Because the technical foundation already exists, the binding constraint is procedural accountability. The policy implication is that digital maturity does not automatically produce credible reporting; governance formalization remains necessary.

Under this scenario, organizations should first identify the events that materially affect recognition credibility. These commonly include data acquisition from external parties, customer-consent verification, approval of de-identification or anonymization routines, validation of enrichment models, designation of beneficial-use cases, and authorization of capitalization or disclosure. Each event should be tied to responsible roles and time-stamped evidence. External auditors should be granted read access to these event layers rather than only to final reports. Regulators, where appropriate, may specify minimum event categories that firms must retain for inspection. When firms take this approach,

ISSN: 3068-7462 https://doi.org/10.63646/jeagf.2025.030201

blockchain operates as a process-control reinforcement mechanism rather than a substitute for ERP or data-lake infrastructure.

5.2 Scenario Two

Fragmented ecosystems and multi-party dependence. A second scenario arises when data assets are co-created across firms, suppliers, platforms, logistics partners, cloud vendors, and analytics providers. Here, the central problem is not internal sequencing alone but inter-organizational fragmentation. Supply-chain studies repeatedly show that blockchain creates value when provenance, handoffs, and shared accountability are otherwise difficult to verify (Treiblmaier, 2018; Wang et al., 2019; Wamba et al., 2020; Sahoo et al., 2024). The same logic applies to enterprise data assets created through ecosystems. Customer-behavior datasets, industrial telemetry, marketplace records, and service logs often pass through many actors before they become analytically useful. If recognition relies on ecosystem data, the focal firm must demonstrate not only technical possession but also lawful rights, transformation legitimacy, and evidentiary continuity across partners.

In this scenario, consortium blockchains become more attractive than purely private systems (Table 4). Consortium arrangements allow selected partners to validate event records while maintaining differentiated permissions. The crucial design issue is governance standardization: common metadata schemas, shared definitions of custody transfer, harmonized timestamp standards, and clear protocols for dispute resolution. Smart contracts may record who supplied data, under what license, whether quality checks were passed, and whether downstream reuse remains within contractual bounds. External assurance providers can then verify ecosystem continuity without requiring unrestricted access to commercially sensitive content. Strategic policy should therefore focus on standard-setting and node governance. Without standardization, a consortium blockchain merely reproduces fragmentation in a new technical form.

Table 4. Policy scenarios and recommended governance paths

Scenario	Behavioral pattern	Strategic risk	Recommended policy path
Low maturity / low interdependence	Conventional internal controls dominate	Overinvestment in complex infrastructure	Adopt selective blockchain modules only where verification cost is high
Medium maturity / contested rights	Recognition disputes and inconsistent audit evidence	Escalating governance friction	Implement provenance logs and permissioned auditor access first
High maturity / ecosystem exchange	Frequent data sharing across firms and authorities	Information asymmetry across organizational boundaries	Use consortium governance, smart controls, and synchronized reporting
High opportunism / weak sanctions	Manipulation remains attractive	Blockchain becomes symbolic rather than disciplinary	Strengthen reward-penalty design and embed automated exception triggers

5.3 Scenario Three

High regulatory pressure and low trust. A third scenario appears in sectors where regulators, investors, or public stakeholders are highly sensitive to data misuse, privacy violations, or opaque asset claims. Healthcare, critical infrastructure, finance, and public-sector data exchanges are common examples. In these settings, the legitimacy value of blockchain may be as important as its operational value. Studies in healthcare information management and IoT show that blockchain improves trust when records must be auditable, yet access must remain controlled (Prybutok et al., 2022; Adere, 2022; Mamun et al., 2022). For data-asset recognition, this means that regulators may be more willing to accept digital reporting claims when a firm can show immutable evidence trails for rights management, processing approvals, and post-recognition monitoring.

However, strong regulatory pressure also raises the risk of overengineering. Organizations may respond by storing too much, disclosing too broadly, or layering blockchain onto immature governance processes simply to demonstrate compliance effort. That can backfire by increasing cost, privacy exposure, and operational complexity. A more effective strategy is minimal sufficiency: record only those governance events that matter most for assurance and regulatory review. Firms should implement role-based access, cryptographic proofs, and off-chain confidential storage, while exposing standardized evidence summaries to auditors and supervisors. Regulators, in turn, should avoid technology mandates that prescribe specific vendors or architectures. Their role is better framed as defining evidence requirements, interoperability expectations, and accountability rules. This balances innovation with comparability.

5.4 Scenario Four

Strong technology, weak audit capability. A recurrent practical problem is that firms may implement sophisticated blockchain or data-governance tools while assurance providers remain unable to audit them effectively. Han et al. (2023), Schmitz and Leoni (2019), and Liu et al. (2019) all imply that professional competence is a limiting factor in blockchain-enabled accounting. If auditors lack expertise in permission models, smart-contract logic, key management, and data-lineage interpretation, the mere existence of immutable logs may not improve assurance quality. Worse, technological opacity can generate superficial confidence. The resulting risk is governance theater: systems appear rigorous, but audit conclusions still rely on managerial narratives because auditors cannot meaningfully test the architecture.

The policy path for this scenario is capability co-development (Figure 3). Firms should involve internal and external auditors during design rather than after deployment. Audit trails must be built with testability in mind, including readable event labels, standardized exception handling, preserved version history, and controlled access to supporting off-chain evidence. Professional bodies and regulators should update audit guidance to cover blockchain-enabled recognition workflows, including how to evaluate smart-contract controls, data-lineage integrity, and the continuing validity of recognized digital assets. Universities and executive training providers should also update AIS curricula to address hybrid architectures that combine blockchain, ERP, cloud infrastructure, and analytics

governance. Without such capability development, the system-level promise of blockchain remains under-realized.

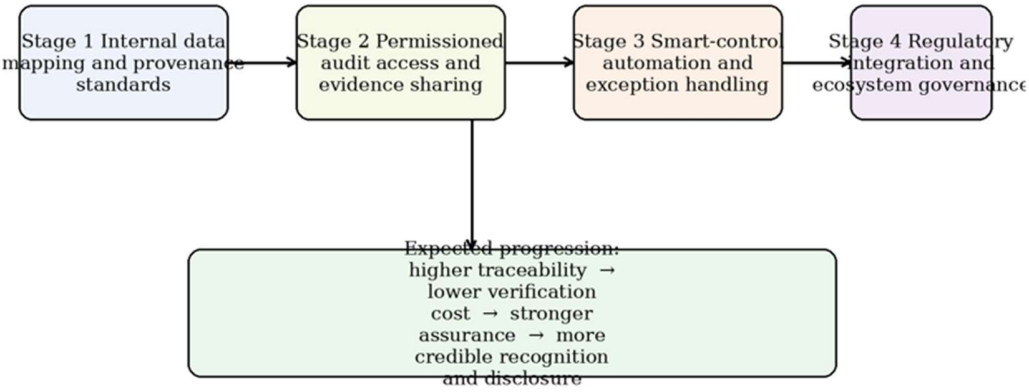

Figure 3. Strategic policy path for blockchain adoption in data-asset governance

5.5 Strategic Policy Path One

Defining recognition ontology before choosing technology. The first strategic path is conceptual clarity. Firms often rush toward dashboards, ledgers, or tokenized representations before defining the ontology of the asset itself. A recognition ontology should specify what counts as the asset boundary, what rights are included, what quality dimensions matter, what evidence is needed to demonstrate future benefit, and what events can invalidate the claim later. Shared-ledger systems are only as useful as the ontology they operationalize. If the underlying asset definition is vague, blockchain merely preserves ambiguity. Therefore, standard setters and industry bodies should work toward domain-sensitive recognition ontologies for data assets, allowing flexibility in valuation while standardizing provenance and rights documentation.

5.6 Strategic Policy Path Two

Designing hybrid architectures around assurance-critical events. The second path is architectural pragmatism. Organizations should not attempt to place entire datasets or all processing histories on chain. Instead, they should identify assurance-critical events and anchor those events cryptographically. Examples include acquisition approvals, model-release decisions, privacy-impact reviews, valuation signoffs, impairment triggers, and disposal authorizations. Off-chain repositories remain the primary environment for data storage and analysis; the blockchain layer serves as a trusted registry of governance events. This approach lowers cost, improves scalability, and respects confidentiality while still producing auditable continuity. It also aligns with findings from ERP and supply-chain integration studies that blockchain works best when targeted at specific coordination failures rather than generalized as a universal database (Dasaklis et al., 2021; Sunmola & Lawrence, 2024; Wong et al., 2020).

5.7 Strategic Policy Path Three

Aligning incentives through visibility, not only penalties. The uploaded article rightly emphasized the importance of incentive and penalty design. In the present framework, that

insight is retained but broadened. Incentives should not be reduced to fines, subsidies, or formal sanctions alone. Visibility itself changes incentives. When event histories are harder to alter, when exceptions are permanently logged, and when approvals are attributable to named roles, the cost of opportunism rises even before external punishment occurs. Organizations should therefore design systems that make governance choices observable to appropriate reviewers. This includes dashboards for unresolved exceptions, mandatory rationales for overrides, and automatic alerts when post-recognition events undermine the continuing validity of an asset. Such visibility-based governance is often more sustainable than high-intensity punishment because it embeds accountability into routine operations.

5.8 Strategic Policy Path Four

Embedding post-recognition stewardship into the reporting cycle. Traditional accounting often treats recognition as the culmination of control. For data assets, recognition is only the midpoint. Value may fall if data age rapidly, if customer consent is withdrawn, if model inputs drift, if security incidents occur, or if regulation changes. Blockchain can strengthen governance only when post-recognition stewardship is embedded in the reporting cycle. This means that usage records, access changes, retraining events, legal restrictions, and impairment indicators should continue to generate accountable events after recognition. Audit committees should review these events regularly, and reporting systems should support impairment or disclosure updates when thresholds are crossed. In effect, data-asset governance must become lifecycle governance. This is where blockchain's persistent event history is particularly valuable.

5.9 Strategic Policy Path Five

Using blockchain to support institutional learning. Finally, blockchain should be understood as a learning infrastructure. Because event histories are preserved over time, organizations can analyze where recognition failures originate, which approval stages generate the most overrides, where audit disputes emerge, and how different governance patterns affect disclosure credibility. Regulators can learn which metadata fields are most informative and which standards are difficult to implement consistently. Auditors can refine testing approaches by studying recurring control failures. Platform teams can identify where interoperability problems break the evidence chain. Thus, the long-term value of blockchain in this area may lie as much in institutional learning and standard refinement as in immediate control benefits. Firms that treat the ledger as a dynamic governance memory rather than a static compliance tool are more likely to achieve lasting value.

6. Discussion

The analysis has several theoretical implications. First, it suggests that the emerging literature on data assets should be integrated more explicitly with enterprise information systems theory. Much of the current debate treats data assets as objects of accounting recognition or legal control, but the evidence reviewed here shows that recognition credibility is inseparable from socio-technical design. Provenance, rights management, access control, transformation logging, and post-recognition stewardship are all system-

enabled processes. The relevant research question is therefore not only whether a dataset meets recognition criteria, but how information systems produce the evidence that makes such criteria assessable. This broadens the focus from valuation mechanics to governance architecture.

Second, the paper refines how blockchain should be theorized in accounting and information systems. A recurring weakness in literature is the tendency to describe blockchain through genetic traits such as immutability, decentralization, and transparency without specifying the organizational mechanisms through which these traits matter. The present article argues that blockchain contributes by converting recognition from a retrospective document exercise into a sequence of accountable events. Its real value lies in synchronizing process evidence across actors who possess partial information and imperfect trust. This mechanism is consistent with supply-chain and ERP research, yet it has force in the data-asset setting because intangible assets are easy to manipulate when process history is opaque.

Third, the paper adds nuance to the relationship between automation and professional judgment. Smart contracts can enforce procedural checkpoints, but they cannot eliminate the interpretive work involved in deciding whether data are legally usable, economically beneficial, or impaired. This means that future research should resist both extremes: the belief that human judgment can be replaced by code, and the opposing belief that code adds little because judgment remains necessary. The more productive position is that automation and judgment are complementary. Blockchain and smart contracts can stabilize evidence creation and approval sequencing, while human experts interpret ambiguous cases and redesign rules as conditions change. This complementarity should become a central theme in future studies of digital accounting infrastructures.

The practical implications are equally clear. For managers, the paper shows that credible data-asset recognition begins with governance design rather than capitalization strategy. Firms need cross-functional arrangements that connect data governance, finance, cybersecurity, legal review, and system administration. Recognition committees for major data assets may be appropriate, especially where datasets are strategically material or heavily regulated. For auditors, the paper implies a shift from document sampling toward process-oriented assurance, with greater attention to lineage evidence, permission structures, and the logic encoded in smart contracts. For regulators, the key lesson is that comparability requires minimum evidence standards, not necessarily uniform technology mandates. What should be standardized are provenance fields, approval events, valuation assumptions, and post-recognition stewardship expectations.

There are also important implementation cautions. Blockchain projects often fail when organizations overstate what technology can accomplish or ignore the cost of integration. Hybrid architecture, metadata discipline, and interoperability with ERP and reporting systems are more important than rhetorical commitments to decentralization. Moreover, governance failures may persist if political incentives remain distorted. A firm that is determined to overstate a digital asset can still feed poor-quality information into an otherwise sophisticated ledger. Thus, blockchain must be accompanied by separation of

duties, independent review, and clear consequences for override abuse. The lesson is not that technology is weak; it is that governance is cumulative. Strong digital controls amplify good institutions and expose weak ones more quickly.

The study has limitations. It is conceptual and synthetic rather than empirical, and it does not test the propositions through interviews, archival data, or simulation. It also focuses on enterprise settings where data assets are sufficiently material to justify complex governance systems; smaller organizations may require simpler approaches. In addition, legal treatment of data ownership and capitalization varies across jurisdictions, meaning that the framework should be adapted to local reporting and data-protection regimes. These limitations point to promising directions for future research. Scholars could examine blockchain-based recognition pilots longitudinally, compare assurance outcomes in firms with and without event-centric governance, or investigate how different industries define the ontology of data assets. They could also test whether blockchain-enabled evidence changes investor trust, auditor behavior, or regulatory outcomes. Such work would extend the conceptual contribution developed here into a more mature empirical research program.

A further implication concerns the organizational conditions required for blockchain-enabled governance to work in practice. Literature often emphasizes technical properties such as immutability, consensus, or smart-contract automation, but enterprise deployment depends on much more mundane factors, including role clarity, cross-functional ownership, data stewardship, process redesign, and the willingness of accountants, auditors, legal teams, and information-system architects to share a common control vocabulary. Without those organizational foundations, the ledger may record events faithfully while the underlying recognition criteria remain ambiguous. In that sense, the governance of data assets is not solved by code alone. It is solved when technological traceability and institutional accountability are jointly embedded in routines, controls, and incentive systems.

This study also highlights an important boundary condition: blockchain should not be interpreted as a universal replacement for all existing accounting, assurance, or compliance infrastructures. In some low-complexity environments, conventional databases with robust access controls, documented valuation policies, and standardized audit procedures may already provide sufficient assurance at lower cost. Blockchain becomes strategically valuable when the organization faces repeated data exchanges across units or firms, contested rights, heterogeneous information sources, high verification costs, or material risks of opportunism. The policy implication is therefore selective adoption rather than technological maximalism. Regulators and managers should diagnose governance complexity first and then decide the degree of ledgerization, automation, and external disclosure that is proportionate to the problem.

7. Conclusion

This paper develops an original review-based governance article on the recognition of enterprise data assets in information systems and argues that blockchain is best understood not as an isolated technology, but as a governance infrastructure capable of restructuring

how data-related claims are created, verified, and supervised. By following the logical architecture of the source manuscript while building a distinct argument, the study first shows why data assets generate persistent recognition problems: value is context dependent, control rights are fragmented, reuse is easy, and conventional accounting systems often cannot document provenance, legitimacy, and transformation histories with sufficient granularity. These conditions create room for inflated valuation, repeated capitalization, selective disclosure, auditor dependence, and fragmented regulation.

The article then synthesizes the literature on blockchain, accounting information systems, audit digitalization, enterprise integration, and multi-actor governance to explain why distributed ledgers matter in this context. The core contribution is conceptual rather than purely technical. Blockchain can support data-asset recognition when it records the provenance of datasets, timestamps transformations, documents access rights, connects audit evidence to process events, and creates a shared control layer among firms, auditors, and regulators. In other words, blockchain provides value when it turns an opaque recognition process into a traceable governance process. This shift from static reporting to process-based assurance is the main theoretical move advanced in the paper.

A second contribution lies in the multi-actor perspective. The paper shows that the governance of data assets cannot be reduced to the internal behavior of firms alone. Recognition outcomes are shaped by the strategic interaction of at least three actor groups: firms seeking flexibility and strategic advantage, auditors seeking revenue and professional legitimacy, and regulators seeking credible market order while managing enforcement costs. Once these interdependencies are made explicit, the governance problem becomes one of incentive alignment. Rewards for compliant recognition, sanctions for manipulation, standards for evidence traceability, and transparent access rules for audit and supervision all influence whether blockchain-enabled governance produces genuine accountability or merely a new technical façade.

Third, the paper offers a staged policy path for implementation. Rather than recommending full-scale mandatory adoption, it proposes a gradual model in which organizations begin with internal provenance controls, proceed to permissioned audit access, and only then move toward wider inter-organizational or regulatory integration. This staged approach is especially important for resource-constrained organizations and for jurisdictions where data-property rules, valuation standards, and digital-audit competencies remain immature. For such contexts, the most practical strategy is to build limited but credible blockchain-supported control modules around high-value datasets, sensitive disclosure areas, or inter-firm data exchanges. Over time, these modules can become the foundation for broader governance architecture.

The study further suggests that the quality of blockchain-enabled governance depends on four conditions. First, recognition criteria must be explicitly defined, including the distinction between raw data, processed datasets, derivative data products, and analytically enhanced assets. Second, control rights and usage rights must be documented in ways that can be linked to system events and contractual arrangements. Third, auditors must be granted reliable but proportionate access to verifiable evidence without compromising

privacy or trade secrecy. Fourth, regulators should combine technological standards with differentiated incentives and penalties so that the expected payoff from compliance exceeds the expected payoff from opportunism. When these conditions are absent, blockchain may improve data storage or coordination but will not solve the deeper recognition problem.

There are also clear limitations. This article is a conceptual and integrative study rather than an empirical test based on field data, archival accounting records, or simulation outputs. It does not estimate the causal effect of blockchain adoption on recognition quality, audit efficiency, or enforcement outcomes. Nor does it resolve all valuation questions associated with data assets, especially in settings where future economic benefits are highly uncertain or where datasets are jointly created across ecosystems. Future research should therefore move in three directions: first, comparative case studies of organizations experimenting with blockchain-supported data accounting; second, formal modeling or simulation of multi-actor incentive structures under alternative regulatory designs; and third, empirical investigation of how industry context, firm size, and digital maturity influence the feasibility of ledger-based assurance.

Despite these limitations, the article advances a clear conclusion. The recognition of data assets is becoming a central challenge of digital-era enterprise governance, and existing accounting and regulatory mechanisms are often too fragmented to provide credible assurance on their own. Blockchain does not remove the need for judgment, standards, or institutional oversight, but it can materially strengthen them by making critical events, rights, and transformations more visible, verifiable, and governable. The future of data-asset recognition will therefore depend less on whether organizations possess blockchain in a narrow technical sense and more on whether they can integrate blockchain into a broader architecture of accountability that combines information systems design, audit logic, and public-interest regulation.

From a managerial standpoint, the paper therefore recommends that organizations treat data-asset recognition as a governance program rather than a narrow reporting exercise. Senior leadership should establish cross-functional steering groups, create evidence standards for data provenance and transformation, identify high-risk recognition points, and align internal audit, legal, IT, and finance teams around a common decision architecture. Such measures are especially important for mid-sized universities, regional enterprises, healthcare networks, industrial firms, and platform businesses whose data assets are economically significant, but whose governance infrastructures remain uneven. In these settings, blockchain-enabled recognition can become a practical route to higher transparency, better accountability, and more reliable digital value creation.

AKNOWLEDGEMENT

The authors acknowledge the constructive intellectual influence of the uploaded manuscript and the JEAGF manuscript template in shaping the structural design of this article, while all arguments, wording, figures, tables, and synthesis in the present paper are original.

Reference

Abdullah, N. A. H. N., & Almaqtari, F. A. (2024). The impact of artificial intelligence and Industry 4.0 on transforming accounting and auditing practices. Journal of Open Innovation: Technology, Market, and Complexity, 10(4), 100218. https://doi.org/10.1016/j.joitmc.2024.100218

Adere, E. M. (2022). Blockchain in healthcare and IoT: A systematic literature review. Array, 14, 100139. https://doi.org/10.1016/j.array.2022.100139

Akter, S., Kummer, T.-F., & Yigitbasioglu, O. (2024). Looking beyond the hype: The challenges of blockchain adoption in accounting. International Journal of Accounting Information Systems, 52, 100681. https://doi.org/10.1016/j.accinf.2024.100681

Ali, M. H., Chung, L., Kumar, A., Zailani, S., Tan, K. H., & Luthra, S. (2021). A sustainable Blockchain framework for the halal food supply chain: Lessons from Malaysia. Technological Forecasting and Social Change, 170, 120870. https://doi.org/10.1016/j.techfore.2021.120870

Baranwal, G., Pateriya, R. K., Singh, V. K., & Chauhan, V. S. (2023). Secure data sharing and compliance using privacy-preserving computation in data-intensive ecosystems. Journal of Information Security and Applications, 73, 103437. https://doi.org/10.1016/j.jisa.2023.103437

Benzidia, S., Makaoui, N., & Subramanian, N. (2021). Impact of ambidexterity of blockchain technology and social factors on new product development: A supply chain and Industry 4.0 perspective. Technological Forecasting and Social Change, 163, 120819. https://doi.org/10.1016/j.techfore.2021.120819

Bonson, E., & Bednarova, M. (2019). Blockchain and its implications for accounting and auditing. Meditari Accountancy Research, 27(5), 725-740. https://doi.org/10.1108/MEDAR-11-2018-0406

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

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

Chod, J., Trichakis, N., Tsoukalas, G., Aspegren, H., & Weber, M. (2020). On the financing benefits of supply chain transparency and blockchain adoption. Management Science, 66(10), 4378-4396. https://doi.org/10.1287/mnsc.2019.3434

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) (pp. 1-6). IEEE. https://doi.org/10.1109/AICCSA.2016.7945805

Coyne, J. G., & McMickle, P. L. (2017). Can blockchains serve an accounting purpose? Journal of Emerging Technologies in Accounting, 14(2), 101-111. https://doi.org/10.2308/jeta-51910

Da Xu, L., 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

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5-21. https://doi.org/10.2308/isys-51804

Dasaklis, T. K., Voutsinas, T. G., & Mihiotis, A. (2021). Integrating blockchain with enterprise resource planning systems: Benefits and challenges. In Proceedings of the 2021 International Conference on Information Systems and Engineering Management (pp. 192-201). ACM. https://doi.org/10.1145/3503823.3503873

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 7(2), 189-208. https://doi.org/10.1080/23270012.2020.1731721

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K.-L. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, 30(7), 1366-1385. https://doi.org/10.1109/TKDE.2017.2781227

Dubey, R., Bryde, D. J., Foropon, C., Tiwari, M., Dwivedi, Y. K., & Schiffling, S. (2023). Incorporating blockchain technology in information systems research. International Journal of Information Management, 68, 102573. https://doi.org/10.1016/j.ijinfomgt.2022.102573

Faccia, A., & Petratos, P. (2021). Blockchain, enterprise resource planning (ERP) and accounting information systems (AIS): Research on e-procurement and system integration. Applied Sciences, 11(15), 6792. https://doi.org/10.3390/app11156792

Fullana, O., & Ruiz, J. (2021). Accounting information systems in the blockchain era. International Journal of Intellectual Property Management, 11(1), 63-80. https://doi.org/10.1504/IJIPM.2021.113357

Giang, N. T. H., Hung, N. Q., Huy, D. T. N., & Van, P. T. H. (2023). Impacts of blockchain on accounting in the business. SAGE Open, 13(4), 1-15. https://doi.org/10.1177/21582440231222419

Gurtu, A., & Johny, J. (2019). Potential of blockchain technology in supply chain management: A literature review. International Journal of Physical Distribution & Logistics Management, 49(9), 881-900. https://doi.org/10.1108/IJPDLM-11-2018-0371

Haddara, M., Norve, S., & Langseth, M. (2021). Enterprise systems and blockchain technology: The dormant potentials. Procedia Computer Science, 181, 1039-1046. https://doi.org/10.1016/j.procs.2021.01.203

Han, H., Lee, J., Kim, J., & Park, S. (2023). Accounting and auditing with blockchain technology and artificial intelligence: A literature review. International Journal of Accounting Information Systems, 48, 100598. https://doi.org/10.1016/j.accinf.2022.100598

Huerta, E., & Jensen, S. (2017). An accounting information systems perspective on data analytics and Big Data. Journal of Information Systems, 31(3), 101-114. https://doi.org/10.2308/isys-51799

Huo, S., Zhang, M., Liu, Y., & Zhao, Y. (2022). A comprehensive survey on blockchain in industrial Internet of Things: Motivations, research progresses, and future challenges. IEEE Communications Surveys & Tutorials, 24(1), 88-122. https://doi.org/10.1109/COMST.2022.3141490

Kamble, S. S., Gunasekaran, A., Kumar, V., & Belhadi, A. (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

Kitsantas, T., Chytis, E., & Achillas, C. (2022). Exploring blockchain technology and enterprise resource planning system: Business and technical aspects, current problems, and future perspectives. Sustainability, 14(13), 7633. https://doi.org/10.3390/su14137633

Kshetri, N. (2018). 1 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

Lacity, M. C. (2022). Blockchain: From Bitcoin to the Internet of Value and beyond. Journal of Information Technology, 37(4), 307-325. https://doi.org/10.1177/02683962221086300

Lei, H., & Ngai, E. W. T. (2023). Blockchain from the information systems perspective: Literature review, synthesis, and directions for future research. Information & Management, 60(7), 103856. https://doi.org/10.1016/j.im.2023.103856

Lu, Y. (2018a). Blockchain: A survey on functions, applications and open issues. Journal of Industrial Integration and Management, 3(4), 1850015. https://doi.org/10.1142/S242486221850015X

Lu, Y. (2018b). 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

Lu, Y. (2019). 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

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 2008513. https://doi.org/10.1080/17517575.2021.2008513

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 254-269). https://doi.org/10.1145/2976749.2978309

Mamun, M. A. A., Azam, S., & Gritti, M. (2022). Blockchain-based electronic health records management: A comprehensive review and future research direction. IEEE Access, 10, 14829-14853. https://doi.org/10.1109/ACCESS.2022.3141079

Moosavi, J., Naeni, L. M., Fathollahi-Fard, A. M., & Fiore, U. (2021). Blockchain in supply chain management: A review, bibliometric, and network analysis. Environmental Science and Pollution Research, 28, 42480-42521. https://doi.org/10.1007/s11356-021-13094-3

Nofel, E., Alhajj, M., Obeid, N., & Al-Okaily, M. (2024). Integrating blockchain, IoT, and XBRL in accounting information systems: A systematic literature review. Journal of Risk and Financial Management, 17(8), 372. https://doi.org/10.3390/jrfm17080372

Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. Olleros & M. Zhegu (Eds.), Research handbook on digital transformations (pp. 225-253). Edward Elgar. https://doi.org/10.4337/9781784717766.00019

Prybutok, G., Sadeghi, A., Mohammadi, S., & Saed, A. (2022). Theoretical and practical applications of blockchain in healthcare information management. Information & Management, 59(6), 103649. https://doi.org/10.1016/j.im.2022.103649

Rozario, A. M., & Vasarhelyi, M. A. (2018). Auditing with smart contracts. The International Journal of Digital Accounting Research, 18, 1-27. https://doi.org/10.4192/1577-8517-v18_1

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

Sahebi, I. G., Masoomi, B., Ghorbani, S., & Uslu, T. (2022). Modeling the enablers for blockchain technology adoption in renewable energy supply chain. Technology in Society, 70, 101871. https://doi.org/10.1016/j.techsoc.2022.101871

Sahoo, S., Sahu, A. K., Pradhan, S. K., & Jena, S. K. (2024). Blockchain for sustainable supply chain management: Trends and ways forward. Electronic Commerce Research, 24, 489-526. https://doi.org/10.1007/s10660-022-09569-1

Schmitz, J., & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: A research agenda. Australian Accounting Review, 29(2), 331-342. https://doi.org/10.1111/auar.12286

Sunmola, F. T., & Lawrence, A. (2024). Key success factors for integration of blockchain and ERP systems: A systematic literature review. Procedia Computer Science, 232, 612-621. https://doi.org/10.1016/j.procs.2024.01.077

Tandon, A., Kaur, P., Mäntymäki, M., & Dhir, A. (2021). Blockchain applications in management: A bibliometric analysis and literature review. Technological Forecasting and Social Change, 166, 120649. https://doi.org/10.1016/j.techfore.2021.120649

Tijan, E., Aksentijević, S., Ivanić, K., & Jardas, M. (2019). Blockchain technology implementation in logistics. Sustainability, 11(4), 1185. https://doi.org/10.3390/su11041185

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

Uddin, M., Stranieri, A., Gondal, I., & Balasubramanian, V. (2021). A survey on the adoption of blockchain in IoT: Challenges and solutions. Blockchain: Research and Applications, 2(2), 100006. https://doi.org/10.1016/j.bcra.2021.100006

Upadhyay, N., Mukhuty, S., Kumar, V., & Kazançoğlu, Y. (2021). Blockchain technology and the circular economy: Implications for sustainability and social responsibility. Journal of Cleaner Production, 293, 126130. https://doi.org/10.1016/j.jclepro.2021.126130

Venkatesh, V. G., Rathi, S., Patwa, S., & Kumar, A. (2020). System architecture for blockchain based transparency of supply chain social sustainability. Robotics and Computer-Integrated Manufacturing, 63, 101896. https://doi.org/10.1016/j.rcim.2019.101896

Wamba, S. F., & Queiroz, M. M. (2020). Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. International Journal of Information Management, 52, 102064. https://doi.org/10.1016/j.ijinfomgt.2019.102064

Wamba, S. F., Queiroz, M. M., & Trinchera, L. (2020). Dynamics between blockchain adoption determinants and supply chain performance: An empirical investigation. International Journal of Production Economics, 229, 107791. https://doi.org/10.1016/j.ijpe.2020.107791

Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. Supply Chain Management, 24(1), 62-84. https://doi.org/10.1108/SCM-03-2018-0148

Wang, Y., Singgih, M., Wang, J., & Rit, M. (2019). Making sense of blockchain technology: How will it transform supply chains? International Journal of Production Economics, 211, 221-236. https://doi.org/10.1016/j.ijpe.2019.02.002

Weigand, H., Blums, I., & de Kruijff, J. (2020). Shared ledger accounting—Implementing the economic exchange pattern. Information Systems, 90, 101437. https://doi.org/10.1016/j.is.2019.101437

Wong, L.-W., Leong, L.-Y., Hew, J.-J., Tan, G. W.-H., & Ooi, K.-B. (2020). Time to seize the digital evolution: Adoption of blockchain in operations and supply chain management among Malaysian SMEs. International Journal of Information Management, 52, 101997. https://doi.org/10.1016/j.ijinfomgt.2019.08.005

Wu, X., Xiong, H., & Li, Y. (2019). Application of Internet of Things and blockchain technologies to improve accounting information quality. IEEE Access, 7, 151455-151465. https://doi.org/10.1109/ACCESS.2019.2930637

Yadav, S., & Singh, S. P. (2020). Blockchain critical success factors for sustainable supply chain. Resources, Conservation and Recycling, 152, 104505. https://doi.org/10.1016/j.resconrec.2019.104505

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

Yuan, Y., & Wang, F.-Y. (2018). Blockchain and cryptocurrencies: Model, techniques, and applications. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 48(9), 1421-1428. https://doi.org/10.1109/TSMC.2018.2854904

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