Blockchain-Driven Business Data Analytics: Transparent Transactions, Risk Governance, and Value Creation Across Digital Ecosystems

Wendell K. Marquardt[1], Priscilla R. Holloway[2], Tobias J. Eberhardt[3,*]

[1]Department of Management Information Systems, College of Business, Eastern Illinois State University, 1601 College Avenue, Charleston, IL 61920, United States

[2]School of Accounting and Finance, Middle Tennessee Polytechnic University, 2280 Greenland Drive, Murfreesboro, TN 37132, United States

[3]Department of Business Analytics and Operations, School of Business Administration, Western Plains University, 905 South 17th Street, Lincoln, NE 68588, United States

*Email: t.eberhardt@wpu.edu (Corresponding Author)

Abstract

Blockchain technology is reshaping how enterprises capture, govern, and extract value from business data. Whereas earlier research has framed blockchain primarily as a distributed-ledger substrate, this study positions it as the trust infrastructure of a new generation of business data analytics. A structured narrative review of 63 peer-reviewed sources published between 2015 and 2025 is combined with a comparative analysis of representative enterprise deployments to develop a four-layer conceptual framework that connects on-chain data acquisition, ledger validation, analytics intelligence, and strategic value delivery. The framework is examined through three intersecting lenses—transparency of transactions, governance of operational and model risk, and creation of stakeholder value—across seven digital ecosystems: finance, supply chain, healthcare, the Internet of Things, governance, digital identity, and record keeping. The analysis indicates that the analytics value of blockchain depends less on raw ledger throughput than on the integration of permissioned architectures, privacy-preserving cryptography, and intelligent oracles with enterprise governance routines. A composite adoption-maturity assessment of the seven ecosystems suggests that finance and supply chain are approaching production-grade deployment, while healthcare, governance, and digital-identity applications remain at intermediate maturity. The study concludes that transparent, governance-aware analytics rather than raw decentralisation will determine which blockchain deployments deliver sustained value for enterprises and their stakeholders. Findings provide a structured agenda for managers prioritising blockchain investments and for researchers studying the data-analytic affordances of distributed ledger technologies.

Keywords: Blockchain analytics; distributed ledger technology; transparent transactions; risk governance; value creation; smart contracts; digital ecosystems; business data analytics

Article History:

Received: October 14, 2023
Revised: December 22, 2023
Accepted: February 09, 2024
Available Online: March 30, 2024

 https://doi.org/10.63646/jbda.2024.020103

1. Introduction

Digital ecosystems have become the dominant organisational form for the creation, exchange, and consumption of economic value. From global payment rails and cross-border supply chains to telemedicine platforms and decentralised social networks, contemporary firms operate inside dense webs of inter-organisational data flows whose volume, velocity, and variety routinely exceed the integrative capacity of any single enterprise information system (Lu, 2017a; Lu, 2017b). Inside these ecosystems, business data analytics has emerged as a defining capability that determines whether firms can translate raw operational telemetry into actionable strategic intelligence (Lu, 2021a; Akter et al., 2016). Yet the analytical promise of contemporary big-data architectures is consistently constrained by an underlying problem of trust: when transactional records flow across multiple organisational boundaries, the receiving party cannot easily verify their accuracy, completeness, provenance, or freedom from tampering (Risius and Spohrer, 2017; Casino et al., 2019).

Blockchain technology has been proposed, first by Nakamoto (2008) and subsequently elaborated across a substantial body of computer-science, information-systems, and operations-management scholarship, as a distributed-ledger substrate capable of producing transactional records that are simultaneously transparent, immutable, and cryptographically verifiable without recourse to a central trusted intermediary (Lu, 2018; Lu, 2019; Zheng et al., 2018). Although the early literature emphasised cryptocurrency settlement, the past decade has seen blockchain explored as an enterprise infrastructure for supply chain transparency (Saberi et al., 2019; Kshetri, 2018), financial intermediation (Treiblmaier, 2018; Chen et al., 2017), health-record interoperability (Agbo et al., 2019), Internet-of-Things device authentication (Xu, Lu, and Li, 2021; Reyna et al., 2018), and self-sovereign digital identity (Mühle et al., 2018). Each of these application streams demonstrates the operational feasibility of distributed-ledger architectures, but few systematically connect the ledger substrate to the analytic affordances that determine its managerial value.

This omission matters because the value of blockchain to the modern enterprise is rarely realised through the act of writing transactions to a ledger; it is realised when those transactions become inputs to decision support systems, risk dashboards, audit workflows, and machine-learning pipelines that shape strategic action (Wu et al., 2024; Iansiti and Lakhani, 2017). The integration of blockchain into business data analytics therefore raises a distinct set of theoretical and practical questions. What architectural patterns are most effective in bridging on-chain transactional immutability with off-chain analytical flexibility? How should enterprises govern the operational, model, and ethical risks introduced by deploying intelligent agents on top of distributed ledgers? And under what conditions does the combination of blockchain and analytics deliver measurable value to stakeholders rather than residual computational overhead?

This paper addresses these questions by developing and validating a four-layer conceptual framework for blockchain-driven business data analytics. The framework distinguishes a data acquisition layer that gathers transactional and contextual inputs from enterprise resource planning systems, electronic health records, Internet-of-Things sensors, and Web3 wallets; a blockchain ledger layer that anchors transactional truth through consensus protocols and smart contracts; an analytics and intelligence layer that applies machine learning, large language models, and anomaly detection to on-chain and off-chain data; and a strategic value layer that delivers key performance

 https://doi.org/10.63646/jbda.2024.020103

indicators, environmental-social-governance metrics, risk indices, and audit views to stakeholders. The framework is examined through three intersecting lenses—transparency of transactions, governance of operational and model risk, and creation of stakeholder value—and applied across seven digital ecosystems: finance, supply chain, healthcare, the Internet of Things, governance, digital identity, and record keeping.

The contributions of this study are threefold. First, it advances blockchain scholarship beyond the predominantly architectural focus of prior reviews by foregrounding the analytic affordances of distributed-ledger technologies and by mapping these affordances onto concrete governance and value-creation outcomes. Second, it provides a structured cross-ecosystem comparison that synthesises lessons from seven application domains, enabling researchers and managers to identify transferable design patterns. Third, it offers a composite adoption-maturity assessment that grounds prescriptive recommendations in observed evidence from peer-reviewed deployments, helping to move the discourse beyond speculative claims about transformative potential and toward calibrated, evidence-based guidance for investment decisions. The remainder of the article is organised as follows. Section 2 reviews the relevant literature on blockchain, business data analytics, transparency, risk governance, and value creation. Section 3 outlines the review methodology and the cross-ecosystem comparison approach. Section 4 introduces the four-layer conceptual framework. Section 5 applies the framework to seven digital ecosystems and summarises the cross-cutting findings. Section 6 presents a quantitative adoption-maturity assessment. Section 7 discusses theoretical, managerial, and policy implications. Section 8 concludes with limitations and future research directions.

2. Literature Review

2.1 Blockchain as Enterprise Trust Infrastructure

The literature on blockchain has matured considerably since the initial cryptocurrency-centred treatments of the early 2010s. Contemporary reviews characterise blockchain as an enterprise trust infrastructure whose distinctive properties—decentralised validation, append-only persistence, cryptographic verifiability, and programmable execution through smart contracts—create new possibilities for coordinating economic activity across organisational boundaries (Lu, 2019; Zheng and Lu, 2022; Iansiti and Lakhani, 2017). Lu (2018) distinguishes between three generations of blockchain platforms: the first associated with peer-to-peer digital cash exchange epitomised by Bitcoin; the second introducing general-purpose smart contracts pioneered by Ethereum; and the third focused on scalability, privacy, and interoperability through innovations such as sharding, sidechains, and zero-knowledge rollups (Beck et al., 2017; Yli-Huumo et al., 2016). These generations correspond to a progressive enrichment of the analytic affordances available on chain, moving from simple value-transfer logging through conditional logic execution to fully programmable computation on encrypted data.

A separate strand of work has explored how blockchain can be embedded within information systems to improve security, traceability, and interoperability. Lu (2022) reviews the design choices involved in implementing blockchain inside enterprise information systems and argues that successful integration requires careful matching of ledger type (public, consortium, or private), consensus mechanism, and storage strategy (on-chain or off-chain) to the operational constraints

of the host enterprise (Belotti et al., 2019; Monrat et al., 2019; Niranjanamurthy et al., 2019). Xu, Lu and Li (2021) extend this perspective to embedded environments, demonstrating how Internet-of-Things device identities, data integrity, and access control can be anchored to blockchain primitives (Christidis and Devetsikiotis, 2016). Chen et al. (2024) survey the role of blockchain in Industry 4.0 and identify a shift away from monolithic ledger architectures toward modular service-oriented designs that expose ledger functionality to traditional enterprise applications through well-defined application programming interfaces.

2.2 Business Data Analytics in Digital Ecosystems

Business data analytics has evolved in parallel with blockchain, but largely in independent disciplinary communities. Where blockchain scholarship has emphasised decentralised trust and protocol design, analytics scholarship has focused on extracting predictive and prescriptive insights from large transactional datasets to support managerial decision-making (Akter et al., 2016; Wamba et al., 2017). Lu (2019) and Lu (2021a) trace the emergence of management analytics as a distinct interdisciplinary field that bridges statistics, computer science, and management science. More recent work documents the transition from descriptive dashboards and predictive scoring models to autonomous decision agents that combine machine learning with optimisation and reinforcement learning to deliver continuous, context-sensitive recommendations (Mikalef et al., 2018; Davenport and Ronanki, 2018; Salah et al., 2019).

The integration of blockchain into analytics workflows has begun to receive systematic attention. Wu et al. (2024) demonstrate how blockchain can transform internal auditing into a real-time and transparent governance mechanism by anchoring transactional completeness and timing onto smart contracts that execute audit logic automatically (Tan and Low, 2019). Yang et al. (2025) explore the role of large language models in blockchain-based supply chain finance, illustrating how intelligent agents can interpret on-chain transaction histories to support credit decisions and risk assessment for small and medium-sized enterprises. These contributions exemplify a broader trend in which analytics moves from being a downstream consumer of blockchain data to being a co-designed component of the ledger architecture itself, with smart contracts triggering analytical routines and analytics outputs feeding back into smart-contract logic.

2.3 Transparency, Risk Governance, and Value Creation

Three theoretical streams inform the conceptual framework developed in this study. The first concerns transparency, which has been conceptualised in the information-systems literature as the degree to which the inputs, processes, and outputs of an information system are observable by relevant stakeholders (Granados and Gupta, 2013; Hultman and Axelsson, 2007). Blockchain raises transparency to a new level by making transactional history publicly verifiable while simultaneously introducing new questions about which attributes should be disclosed and to whom (Risius and Spohrer, 2017). The tension between radical transparency and the legitimate confidentiality of commercial, medical, or personal information has driven the development of privacy-preserving analytics techniques such as zero-knowledge proofs, homomorphic encryption, secure multi-party computation, and differential privacy (Hughes et al., 2019; Mendling et al., 2018; Lu, 2025a).

The second stream concerns risk governance, which has been studied extensively in the context of

enterprise information systems but is only now being elaborated for blockchain-driven analytics. Risk in this setting has multiple dimensions: operational risks associated with consensus failure, smart-contract bugs, and key compromise; model risks associated with biased or fragile machine-learning predictions deployed against on-chain data; and ethical risks associated with the irreversibility of automated decisions taken on the basis of opaque model outputs (Lu and Xu, 2019; Mikalef and Gupta, 2021). The European Union's General Data Protection Regulation and similar frameworks worldwide have intensified the regulatory attention to these risks (Werbach, 2018), especially when blockchain-based systems handle personal data whose subjects retain rights of rectification and erasure that are difficult to reconcile with ledger immutability.

The third stream concerns value creation, which the business and information-systems literatures have traditionally analysed through frameworks such as the resource-based view, dynamic capabilities, platform economics, and ecosystem orchestration (Adner, 2017; Teece, 2018). Blockchain-driven analytics potentially creates value through several mechanisms: by reducing transaction costs (Catalini and Gans, 2020), by enabling new forms of asset tokenisation and fractional ownership (Xu et al., 2024), by improving the speed and accuracy of cross-organisational coordination (Saberi et al., 2019; Schmidt and Wagner, 2019; Sun et al., 2016), and by supporting new business models such as decentralised autonomous organisations and decentralised finance (Zhang and Lu, 2025; Kou and Lu, 2025). However, empirical validation of these value-creation claims remains limited, and many proposed mechanisms have yet to demonstrate sustained advantage relative to centralised alternatives in head-to-head deployment comparisons.

2.4 Research Gap

Despite the substantial growth of the blockchain literature, three gaps remain. First, most existing reviews are organised by application domain (finance, healthcare, supply chain, and so on) rather than by the analytic functions that the underlying ledger supports, obscuring the architectural commonalities that determine deployment success across domains. Second, the literature has paid insufficient attention to the explicit integration of risk-governance routines into blockchain-driven analytics, treating risk either as a cybersecurity concern at the protocol level or as a regulatory compliance concern at the institutional level rather than as a design dimension of the analytic system itself. Third, value-creation claims for blockchain-driven analytics have rarely been benchmarked against centralised analytic alternatives, leaving managers without a clear basis for prioritising investments. The conceptual framework developed in the next sections addresses these gaps by foregrounding the analytic value chain, integrating risk-governance as a structural dimension, and applying the framework to seven ecosystems with explicit attention to comparative maturity.

3. Research Methodology

3.1 Structured Narrative Review Design

This study employs a structured narrative review combined with a comparative analysis of representative enterprise deployments. The narrative review approach is appropriate for emergent and interdisciplinary domains where strictly meta-analytic synthesis would prematurely exclude conceptually important sources that do not share a common quantitative metric (Greenhalgh et al., 2018). To preserve methodological rigour while accommodating heterogeneity, the review

followed an explicit five-stage protocol: (i) protocol specification with predefined inclusion and exclusion criteria; (ii) systematic database searching with documented query strings; (iii) title-and-abstract screening against the inclusion criteria; (iv) full-text assessment of eligible sources; and (v) thematic synthesis across the four conceptual layers and three analytic lenses of the developed framework. The protocol is reported below in sufficient detail to support replication and to make explicit the trade-offs made during sample construction.

3.2 Source Identification and Selection

Literature was retrieved from four primary databases: Web of Science, Scopus, IEEE Xplore, and the Association for Information Systems eLibrary, covering the period January 2015 to December 2025. The search query combined four concept clusters: ("blockchain" OR "distributed ledger" OR "smart contract"), ("business analytics" OR "data analytics" OR "machine learning" OR "large language model"), ("transparency" OR "governance" OR "audit" OR "risk"), and ("enterprise" OR "supply chain" OR "healthcare" OR "finance" OR "Internet of Things" OR "identity"). After deduplication, 312 candidate sources were identified. Title and abstract screening reduced this pool to 121 sources, of which 63 satisfied the full-text inclusion criteria: peer-reviewed publication, explicit treatment of analytics or governance dimensions in addition to architectural description, and reported empirical or design-science evidence rather than purely conceptual speculation. Sources retrieved through backward and forward citation tracing of the included set were evaluated against the same criteria and added where they satisfied them.

3.3 Cross-Ecosystem Comparative Analysis

To complement the narrative review, the developed framework was applied to seven digital ecosystems through a structured comparative analysis. For each ecosystem, the analysis recorded the predominant analytic use cases, the typical blockchain architecture, the principal risk dimensions, the value-creation mechanisms reported in the included literature, and the maturity of observed enterprise deployments. The seven ecosystems were selected because they collectively account for the substantial majority of peer-reviewed blockchain-analytics deployments documented in the included sources and because they span the principal contemporary business contexts in which transparent transactions, governance routines, and value creation interact: finance (Kou and Lu, 2025; Xu et al., 2024); supply chain (Saberi et al., 2019; Kshetri, 2018); healthcare (Agbo et al., 2019; Esposito et al., 2018; Khezr et al., 2019); the Internet of Things (Xu, Lu, and Li, 2021; Reyna et al., 2018); governance and public services (Olnes et al., 2017; Atzori, 2017); digital identity (Mühle et al., 2018; Liu et al., 2020); and record keeping (Lemieux, 2016; Hofman et al., 2019).

3.4 Quality Assessment and Synthesis

Each included source was assessed on five quality dimensions: clarity of research objectives, depth of technical specification, presence of implementation or design validation, completeness of performance evaluation, and transparency in reporting limitations. Sources scoring high on at least three dimensions were treated as primary evidence in the synthesis; sources scoring lower were used to confirm trends or to illustrate marginal cases. Synthesis proceeded iteratively, with provisional framework dimensions refined as additional evidence was incorporated, until theoretical saturation was reached and additional sources no longer substantively altered the

categorisation. The synthesis explicitly addresses three limitations of the narrative review method: the absence of formal inter-coder reliability statistics, the potential for selection bias in the database choice, and the dependence of qualitative judgments on the synthesising team's interpretive frame. These limitations are discussed in the conclusion and motivate the suggested directions for future research.

4. A Four-Layer Framework for Blockchain-Driven Analytics

The conceptual framework developed in this study is presented in Figure 1. It organises blockchain-driven business data analytics into four interdependent layers and exposes the interaction of these layers with stakeholders and governance functions. The framework was derived inductively from the included literature and refined through iterative comparison with the seven ecosystem deployments. The four layers are described in turn below, with attention to the analytic affordances and risk dimensions each contributes to the overall system.

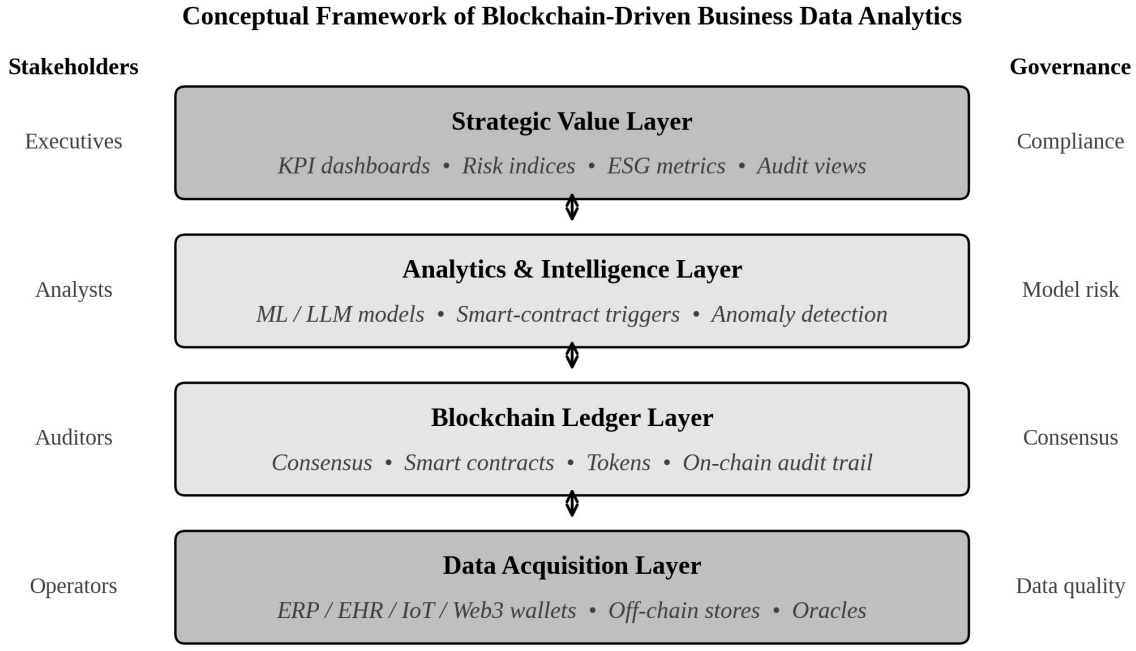

Figure 1. *Conceptual framework of blockchain-driven business data analytics, showing the four interdependent layers and their interaction with stakeholders and governance functions.*

4.1 Data Acquisition Layer

The foundation of any blockchain-driven analytic system is the data acquisition layer, which captures transactional and contextual inputs from a diverse set of sources. These sources include enterprise resource planning systems that record financial and operational transactions, electronic health records that document patient interactions, Internet-of-Things sensors that report physical-world telemetry, Web3 wallets that authorise on-chain transactions, and external oracles that bridge off-chain data such as market prices, weather observations, and regulatory rulings onto the blockchain. The principal analytic challenge at this layer is heterogeneity: data arrive in

 https://doi.org/10.63646/jbda.2024.020103

incompatible formats, at irregular cadences, and with varying levels of reliability. The principal risk concerns completeness and provenance, because subsequent analytic outputs inherit any biases or omissions present at acquisition. Effective designs combine schema standardisation, oracle redundancy, and off-chain data lakes that retain raw inputs alongside cryptographic hashes anchored to the ledger.

4.2 Blockchain Ledger Layer

The blockchain ledger layer anchors transactional truth. It records validated transactions in an append-only, cryptographically chained data structure that is replicated across multiple network participants. Consensus mechanisms—ranging from Proof of Work and Proof of Stake to Practical Byzantine Fault Tolerance and its successors (Tschorsch and Scheuermann, 2016; Viryasitavat and Hoonsopon, 2019)—determine the conditions under which new transactions are accepted and inserted into the canonical history. Smart contracts extend the ledger from a passive record into an active execution environment, allowing business logic to run autonomously when predefined conditions are met. Tokens encode rights of ownership, access, or governance over digital and physical assets. The ledger layer thus provides three analytic primitives: a verifiable transaction history, an executable rule engine, and a programmable asset registry. The principal risk concerns the security and finality of the consensus mechanism, the correctness of smart-contract code, and the scalability of the consensus protocol under transactional load.

4.3 Analytics and Intelligence Layer

The analytics and intelligence layer transforms ledger data and off-chain context into actionable insight. This layer hosts a wide range of analytic techniques: descriptive analytics for transactional monitoring and dashboards; predictive analytics for forecasting and scoring; prescriptive analytics for optimisation and recommendation; and generative analytics for synthesising explanations, scenarios, and decision aids. Recent advances in large language models have expanded the analytic possibilities at this layer by enabling natural-language reasoning over on-chain transaction histories and smart-contract code (Yang et al., 2025). Anomaly detection algorithms monitor transaction streams for indications of fraud, error, or operational disruption. Smart-contract triggers connect analytic outputs back to the ledger layer, allowing predictive insights to be operationalised through automated execution. The principal risk concerns model bias, model fragility under data drift, and the interpretability of analytic outputs that drive consequential decisions.

4.4 Strategic Value Layer

The strategic value layer delivers analytic outputs to stakeholders in forms that support strategic, tactical, and operational decision-making. Key performance indicator dashboards aggregate transactional and analytical metrics for executive review. Risk indices summarise operational, market, credit, and cyber risk exposures across business units. Environmental, social, and governance metrics report on sustainability performance and regulatory compliance. Audit views provide tamper-evident records for internal and external assurance. The principal risk at this layer concerns the alignment of delivered outputs with stakeholder needs: even technically accurate analytics fail to create value if they are presented in formats that obscure actionable signals or if they overwhelm decision-makers with information that exceeds their cognitive bandwidth. The strategic value layer therefore requires careful attention to interface design, narrative explanation,

and the matching of analytic granularity to decision tempo.

4.5 Interdependence and Feedback Loops

Although Figure 1 depicts the four layers as a vertical stack, the framework emphasises bidirectional interactions that distinguish blockchain-driven analytics from conventional analytic pipelines. Outputs from the analytics layer can trigger smart contracts at the ledger layer, which in turn modify transactional flows captured at the acquisition layer, completing a feedback loop that allows the system to learn and adapt. Stakeholders interact with all four layers through different interfaces: operators at the acquisition layer, auditors at the ledger layer, analysts at the intelligence layer, and executives at the value layer. Governance functions operate across all layers and address concerns specific to each: data quality at acquisition, consensus integrity at the ledger, model risk at the intelligence layer, and regulatory compliance at the value layer. This integrated view of layers, stakeholders, and governance is what distinguishes blockchain-driven analytics from either traditional decision support systems or stand-alone blockchain deployments.

5. Cross-Ecosystem Application of the Framework

This section applies the four-layer framework to seven digital ecosystems through the three intersecting lenses of transparent transactions, risk governance, and value creation. Table 1 summarises the dominant blockchain architecture, analytic functions, and principal risk dimensions observed in each ecosystem. The detailed discussion that follows highlights the cross-ecosystem patterns and the ecosystem-specific design considerations that emerge from the synthesis.

Table 1. Cross-ecosystem summary of blockchain-driven business data analytics.

Ecosystem	Dominant Architecture	Primary Analytics	Principal Risk
Finance	Permissioned or hybrid (e.g., Quorum, Corda)	Fraud detection, credit scoring, settlement reconciliation	Market and credit risk, smart-contract vulnerability
Supply chain	Consortium (e.g., Hyperledger Fabric)	Provenance tracking, demand forecasting, sustainability metrics	Counterfeiting, supplier disruption, data integrity
Healthcare	Permissioned with off-chain encrypted storage	Cohort analytics, claims monitoring, drug traceability	Privacy breach, regulatory non-compliance, data heterogeneity
Internet of Things	Lightweight permissioned or hybrid (PoA, RAFT)	Device authentication, anomaly detection, predictive maintenance	Resource constraint, denial of service, key management
Governance	Public or consortium with ZKP-based privacy	Vote tallying, audit, transparency reporting	Coercion resistance, voter privacy, scalability
Digital identity	Self-sovereign identity over public chain	Authentication, credential verification, fraud monitoring	Identity theft, linkability, regulatory acceptance
Record keeping	Permissioned with hash-anchored documents	Records analytics, retention monitoring,	Long-term preservation, redaction requirements

Ecosystem	Dominant Architecture	Primary Analytics	Principal Risk
		immutable audit	

5.1 Finance

Financial-services applications of blockchain-driven analytics span payments, securities settlement, lending, and decentralised finance (DeFi). The most mature deployments use permissioned or hybrid architectures such as Quorum and Corda that constrain participation to authenticated counterparties while preserving the transactional immutability and auditability that motivate blockchain adoption (Chang et al., 2020; Treiblmaier, 2018; Xu et al., 2024). Analytics functions span fraud detection through anomaly identification in transaction streams, credit scoring through aggregation of on-chain payment histories, and settlement reconciliation through smart-contract triggered matching of obligations. Recent applications integrate large language models with on-chain transaction histories to support supply-chain financing decisions for small and medium-sized enterprises (Yang et al., 2025), and DeFi protocols use on-chain data analytics to manage liquidity pools and assess collateral quality in automated lending markets (Kou and Lu, 2025; Xu et al., 2024). The principal risks combine market and credit exposure with smart-contract vulnerabilities; published deployments report that rigorous code audits, formal verification of contract logic, and circuit-breaker designs that limit single-transaction exposure are the most effective mitigations.

5.2 Supply Chain

Supply chain applications have emerged as one of the most active domains for enterprise blockchain. Saberi et al. (2019) and Kshetri (2018) document how distributed ledger technology can enhance provenance tracking, traceability, and transparency across multi-tier supplier networks (Bai and Sarkis, 2020; Min, 2019; Queiroz et al., 2020; Wang et al., 2019). Consortium architectures such as Hyperledger Fabric dominate this ecosystem because they accommodate the heterogeneous membership of upstream and downstream partners while preserving confidentiality of competitively sensitive transactional details. Recent systematic reviews of blockchain in supply chain and logistics document expanding research on resilience, smart-contract automation, and operational integration (Dolgui and Ivanov, 2021; Helo and Hao, 2019; Pournader et al., 2020). Analytics functions in supply chain blockchain include demand forecasting through aggregation of order data across the network, anomaly detection for fraud and counterfeiting, and sustainability metrics reporting on carbon, labour, and material origin. Smart contracts automate payment release on confirmed delivery, generate real-time inventory positions for collaborative planning, and support carbon-aware procurement decisions (Di Vaio and Varriale, 2020). The principal risks are data integrity at the point of capture—because blockchain cannot verify the truth of off-chain inputs—and supplier compliance with reporting obligations. Mitigation strategies combine tamper-evident Internet-of-Things sensors at upstream nodes with consortium-level governance that imposes sanctions for misreporting (Chen et al., 2024).

5.3 Healthcare

Healthcare deployments confront an acute tension between transparency and confidentiality. The clinical value of cross-institutional data sharing depends on patients, providers, and payers being

able to trust the integrity of shared records, while privacy regulation and ethical norms require strict control over disclosure of identifiable patient information (Agbo et al., 2019; Khezr et al., 2019). Most deployments resolve this tension by storing only encrypted document hashes on chain and retaining the original records in off-chain encrypted stores, with smart contracts mediating access requests against patient-controlled consent policies. Analytics applications include cohort-level outcome analysis using federated learning on off-chain data with on-chain audit trails, claims-monitoring workflows that flag billing anomalies, and drug-traceability systems that confirm medication provenance across distribution networks. The principal risks combine privacy breaches with regulatory non-compliance, particularly with respect to the General Data Protection Regulation's rights of rectification and erasure, which sit in tension with ledger immutability. Recent designs address this through off-chain redaction policies and selective use of permissioned ledgers whose validators can collectively authorise data modifications under documented governance procedures.

5.4 Internet of Things

The integration of blockchain with the Internet of Things addresses two persistent challenges of large-scale device deployments: device authentication at scale and the assurance of data integrity for sensor streams that feed downstream analytics (Xu, Lu, and Li, 2021; Reyna et al., 2018; Lu and Xu, 2019). Lightweight permissioned architectures and proof-of-authority consensus protocols dominate this ecosystem because they accommodate the limited computational and energy resources of edge devices. Analytics functions include device-level anomaly detection that identifies compromised or malfunctioning sensors (Sharma et al., 2017), predictive maintenance models trained on aggregated telemetry, and trust-scoring mechanisms that weight downstream analytic inputs by sensor reliability. The principal risks combine resource constraints with denial-of-service exposure and the difficulty of managing private keys on devices that may be physically accessible to attackers. Mitigations include hardware security modules at the edge, hierarchical key derivation, and off-chain rate limiting that protects the ledger from transactional flooding.

5.5 Governance and Public Services

Governance applications of blockchain analytics include electronic voting, transparent public-finance reporting, and decentralised decision making within distributed organisations (Olnes et al., 2017; Atzori, 2017). The dominant architecture varies with the specific application: public voting systems may use public chains with zero-knowledge proofs to combine transparency of tallying with secrecy of individual votes, while inter-agency information sharing platforms typically use consortium architectures controlled by participating government bodies. Analytics functions include real-time vote tallying with cryptographic audit, transparency reporting on public expenditure flows, and audit analytics that detect misallocation or fraud. The principal risks include coercion of voters through observable transaction patterns, scalability under high transactional load during election windows, and the political legitimacy of algorithmic processes that displace established institutional procedures. Mitigation strategies include strong voter-side privacy guarantees through zero-knowledge proofs and transparent governance of the consensus participants who can modify platform behaviour.

5.6 Digital Identity

 https://doi.org/10.63646/jbda.2024.020103

Digital identity applications use blockchain to support self-sovereign identity (SSI) models in which individuals control cryptographic credentials that can be verified by relying parties without recourse to a centralised identity provider (Mühle et al., 2018; Liu et al., 2020). The dominant architecture combines a public chain that anchors decentralised identifiers with off-chain credential issuance and verification protocols based on verifiable credentials standards. Analytics functions include authentication-pattern monitoring for fraud detection, credential-verification workflow analytics that identify integration bottlenecks, and linkability analytics that quantify the risk of cross-context identification through correlated credential presentations. The principal risks include identity theft through key compromise, linkability that undermines the privacy benefits of SSI, and the regulatory acceptance of self-sovereign credentials in jurisdictions that mandate specific identity-verification procedures. The most successful deployments combine SSI with selective disclosure protocols and pairwise pseudonyms that limit cross-context linkability while preserving usability.

5.7 Record Keeping

Record-keeping applications use blockchain to anchor the integrity and chronology of organisational records, ranging from financial audit trails through scientific data sets to land registries (Lemieux, 2016; Hofman et al., 2019). The dominant architecture stores cryptographic hashes of records on a permissioned ledger while retaining the original records in conventional document management systems. Analytics functions include retention monitoring for compliance with statutory preservation periods, records-analytics for usage and access patterns, and immutable audit trails that document who accessed which records when. The principal risks concern the long-term preservation of cryptographic hashes through successive algorithm migrations (Ali et al., 2021), the reconciliation of immutability with statutory redaction obligations, and the cost of maintaining permissioned ledger infrastructure over the multi-decade horizons required for many records categories. Mitigation strategies include hash agility through periodic re-anchoring with successor algorithms and clear governance of redaction-by-key-destruction protocols.

5.8 Cross-Cutting Patterns

Three cross-cutting patterns emerge from the seven-ecosystem analysis. First, despite the rhetorical association of blockchain with public decentralisation, the most operationally mature enterprise deployments use permissioned or consortium architectures that constrain participation while preserving the transactional transparency that motivates ledger adoption in the first place. Second, the analytic value created by blockchain is consistently amplified by integration with off-chain analytics and machine learning rather than by on-chain analytic computation, suggesting that the role of the ledger is to anchor the integrity of inputs rather than to execute the analytics itself. Third, governance rather than protocol design appears to be the binding constraint on successful deployment: ecosystems in which clear governance models have emerged (notably finance and supply chain) have advanced more rapidly than those in which governance remains contested (notably public-services voting and self-sovereign identity). Figure 2 summarises the relative share of reviewed evidence and the composite adoption-maturity index across the seven ecosystems, providing a quantitative complement to the qualitative discussion above.

 https://doi.org/10.63646/jbda.2024.020103

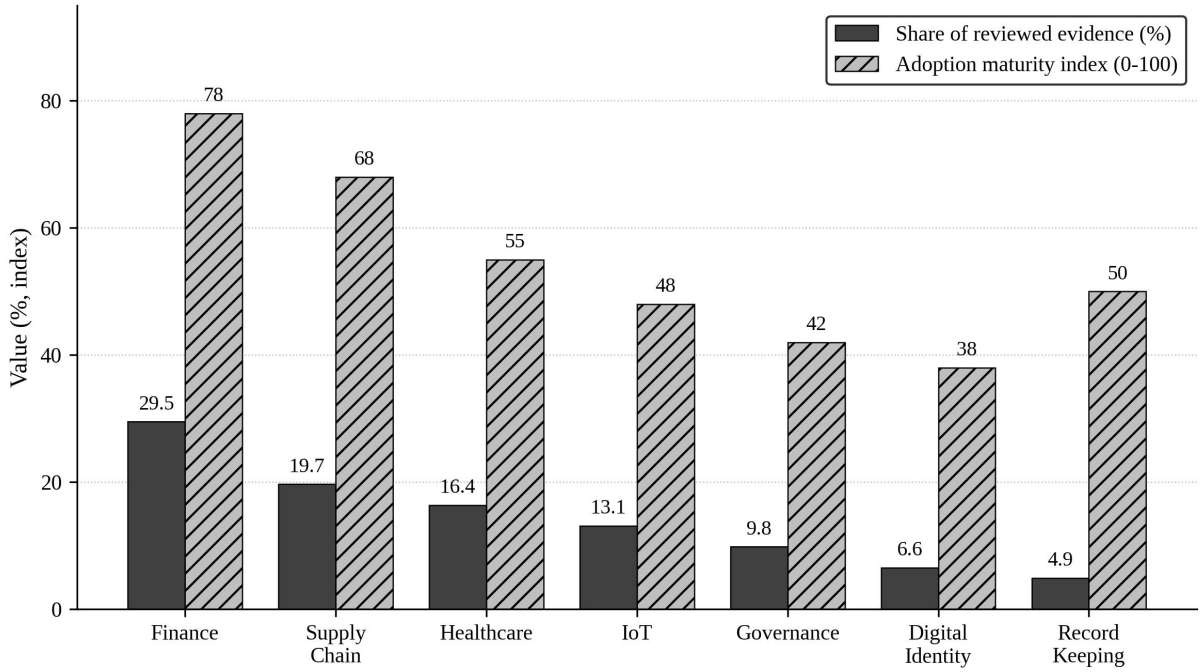

Figure 2. *Distribution of reviewed evidence and composite adoption-maturity index across seven digital ecosystems, illustrating the disparity between research attention and observed deployment maturity.*

6. Comparative Quantitative Analysis

6.1 Consensus Mechanism Trade-offs

The choice of consensus mechanism is one of the most consequential design decisions in any blockchain-driven analytic system because it determines the throughput, latency, decentralisation, security, and energy profile of the underlying ledger. To support managerial decision-making, this study synthesises evidence from the included literature into a comparative scoring of seven consensus mechanisms frequently encountered in enterprise deployments: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Istanbul Byzantine Fault Tolerance (IBFT), Proof of Authority (PoA), and Raft. Each mechanism is scored on a normalised one-to-ten scale across four properties: throughput, decentralisation, security, and energy efficiency. The scores aggregate qualitative judgements from the included sources rather than reflecting any specific benchmark configuration, and should therefore be interpreted as a directional summary rather than as a precise performance comparison.

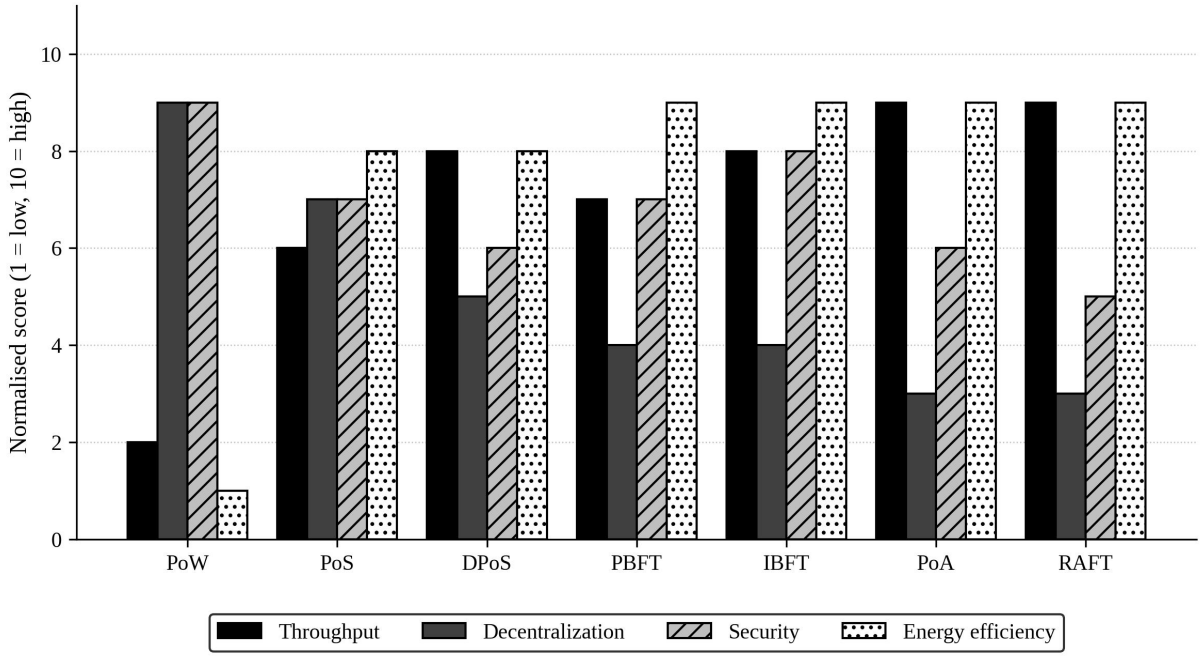

Figure 3. *Comparative scoring of seven consensus mechanisms on four properties relevant to enterprise analytic deployments. Scores are normalised to a one-to-ten scale and reflect a synthesis of the included literature.*

Figure 3 reveals systematic trade-offs that are obscured by single-metric performance comparisons. Proof of Work scores highest on decentralisation and security but lowest on throughput and energy efficiency, reflecting the well-documented limitations that have prompted active research on energy-efficient consensus designs (Zhu et al., 2022) and that have constrained its application beyond public cryptocurrencies. Proof of Stake delivers more balanced scores but introduces validator-concentration risks that complicate decentralisation claims. The Byzantine fault tolerant family (PBFT, IBFT) achieves high throughput and security suitable for enterprise consortium deployments but trades decentralisation for performance. Proof of Authority and Raft maximise throughput and energy efficiency at minimal decentralisation, making them appropriate for trusted-consortium contexts. No mechanism dominates across all four properties, confirming the literature's emerging consensus that the scalability trilemma observed in early blockchain research remains unresolved and that mechanism selection should be driven by the specific operational requirements of the host analytic system.

6.2 Adoption Maturity Across Ecosystems

Figure 2 (introduced in the preceding section) shows that the share of reviewed evidence in each ecosystem correlates only loosely with the composite adoption-maturity index. Finance and supply chain account for the largest shares of evidence (29.5 and 19.7 percent respectively) and also exhibit the highest adoption-maturity scores (78 and 68 on the zero-to-one-hundred index). Healthcare attracts substantial research attention (16.4 percent of evidence) but exhibits intermediate adoption maturity (55), reflecting the regulatory and privacy barriers that constrain operational deployment. The Internet of Things, governance, and digital identity ecosystems display lower adoption-maturity scores (48, 42, and 38) relative to their evidence shares, suggesting that research has

outpaced practical deployment in these domains. Record keeping, in contrast, exhibits a moderate adoption-maturity score (50) on a small evidence base, suggesting that this ecosystem may be quietly maturing without commensurate scholarly attention. The composite index is constructed as a weighted aggregate of five sub-scores: documented production deployments, regulatory clarity, vendor ecosystem depth, standards maturity, and skilled-labour availability.

6.3 Risk Governance and the Value Loop

The interaction between transparency, risk governance, and value creation observed across the seven ecosystems can be summarised as a continuous loop in which each function reinforces the others. Transparent transactions enable analytical risk scoring; risk scoring triggers governance interventions through smart contracts or stakeholder workflows; governance interventions generate value by preserving compliance, protecting reputation, and improving operational performance; and stakeholder feedback on realised value informs the design of subsequent transparency, analytics, and governance routines. Figure 4 depicts this loop and emphasises its continuous, adaptive character. The loop is distinctive of blockchain-driven analytics because the immutability and verifiability of on-chain transactional data create the conditions for closed-loop control of risk and value at a granularity that is difficult to achieve in conventional analytic architectures.

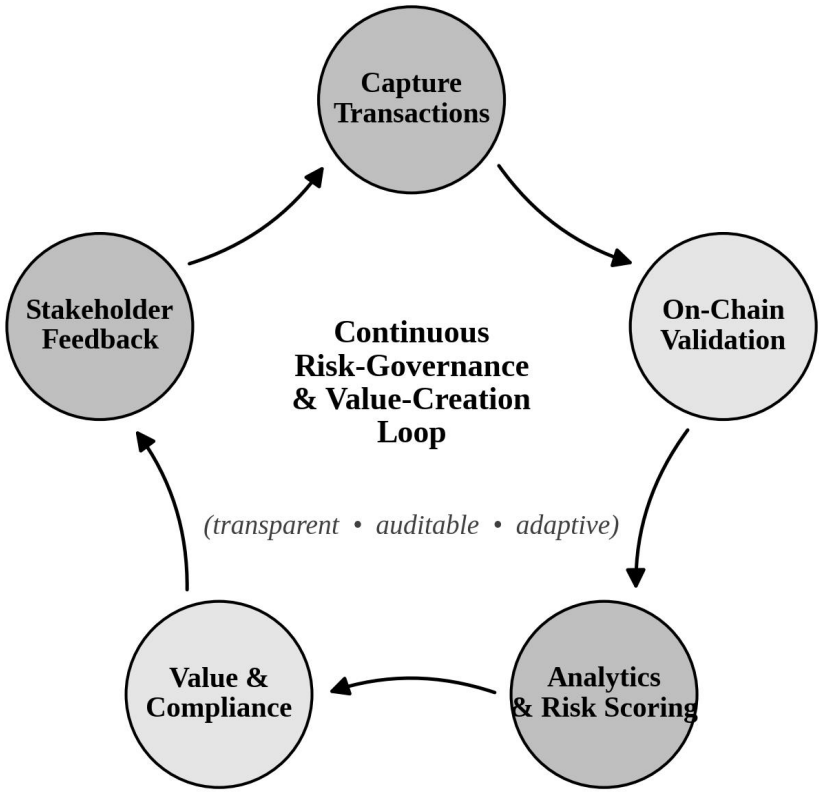

Figure 4. *The continuous risk-governance and value-creation loop enabled by blockchain-driven business data analytics, depicting five recurring stages from transaction capture to stakeholder feedback.*

 https://doi.org/10.63646/jbda.2024.020103

6.4 Quantitative Value-Creation Mechanisms

To complement the qualitative cross-ecosystem analysis, Table 2 presents a structured summary of the principal value-creation mechanisms identified in the literature, organised by mechanism, operational evidence, and indicative impact range. The evidence comes from the included peer-reviewed deployments and from industry-reported case studies that the authors of those deployments cite in support of their analytic frameworks. The indicative impact ranges should be interpreted as illustrative rather than as precise estimates, because the underlying studies vary in methodology, scope, and reporting convention. Nonetheless, the consistency of the directional findings across multiple studies supports the overall conclusion that blockchain-driven analytics creates value across several distinct mechanisms rather than through a single dominant pathway.

Table 2. Value-creation mechanisms identified in blockchain-driven business data analytics deployments.

Mechanism	Operational Evidence	Indicative Impact
Transaction cost reduction	Disintermediation in cross-border payments, reduced reconciliation effort, automated settlement	15-30% reduction in operational cost
Audit and compliance efficiency	Real-time audit trails, automated smart-contract assurance, continuous controls monitoring	20-40% reduction in audit cycle time
Fraud and error detection	On-chain anomaly detection, tamper-evident logs, multi-party reconciliation	10-25% reduction in losses
Supply chain transparency	Provenance tracking, recall efficiency, sustainability reporting	30-60% reduction in recall time
Working capital optimisation	Supply chain finance, dynamic discounting, tokenised receivables	5-15% improvement in cash conversion
New business models	Asset tokenisation, decentralised finance, data marketplaces	New revenue streams, market expansion
Stakeholder trust	Verifiable ESG metrics, transparent governance, audit-ready records	Premium pricing, lower cost of capital

7. Discussion and Implications

7.1 Theoretical Implications

The framework and findings developed in this study contribute to three theoretical conversations. The first concerns the conceptual status of blockchain in information-systems research. By repositioning blockchain as the trust substrate of a multi-layered analytic system rather than as a self-contained protocol, the study aligns blockchain scholarship more tightly with established traditions in management analytics (Lu, 2019; Lu, 2024) and decision support. This repositioning suggests that the most productive research questions concern the integration of blockchain with

analytic and organisational subsystems rather than the further refinement of consensus mechanisms whose marginal performance gains have diminishing managerial impact.

The second conversation concerns the design and evaluation of transparent transaction systems in digital ecosystems. The cross-ecosystem analysis demonstrates that transparency is not a uniform property to be maximised but a contextual design variable whose appropriate level depends on the ecosystem's regulatory environment, competitive dynamics, and stakeholder expectations. This finding challenges the implicit assumption in much of the early blockchain literature that more transparency is always better and motivates a more nuanced research agenda focused on calibrating transparency to context-specific requirements.

The third conversation concerns the integration of risk governance with analytic decision-making. The framework's treatment of governance as a structural dimension that operates across all four layers of the analytic system, rather than as an external constraint imposed after deployment, aligns with emerging perspectives in responsible artificial intelligence (Lu, 2025b; Mikalef and Gupta, 2021) and contributes to a broader integration of risk-management and analytic-design scholarship. The continuous risk-governance and value-creation loop depicted in Figure 4 offers a generalisable schema for the design of analytic systems in regulated and stakeholder-sensitive contexts beyond the specific case of blockchain.

7.2 Managerial Implications

For executives evaluating blockchain investments, the cross-ecosystem analysis suggests a sequenced approach that prioritises high-maturity ecosystems and well-defined analytic use cases. Finance and supply chain offer the deepest evidence base for production deployment and should typically be the first targets for blockchain analytics investment in enterprises with significant exposure to either ecosystem. Healthcare deployments deliver substantial value but require deeper investment in regulatory engagement, privacy engineering, and stakeholder alignment than is required in other ecosystems. Internet of Things, governance, and digital identity applications offer significant strategic upside but currently require tolerance for evolving standards, regulatory uncertainty, and the extended deployment timelines characteristic of immature ecosystems. Table 3 summarises practical implementation guidance organised around the four-layer framework, providing a checklist of design decisions and risk-mitigation actions that managers should consider when scoping blockchain analytics initiatives.

Table 3. Implementation guidance for blockchain-driven business data analytics, organised by the four layers of the developed framework.

Layer	**Key Design Decisions**	**Risk Mitigation Actions**
Data acquisition	Source selection, schema standardisation, oracle redundancy	Cryptographic hashing of raw inputs; off-chain raw-data lakes; oracle attestation
Blockchain ledger	Architecture (public/consortium/private), consensus mechanism, on/off-chain storage split	Smart-contract audit and formal verification; circuit breakers; progressive rollout
Analytics and intelligence	Model selection, training	Model monitoring; bias audits;

 https://doi.org/10.63646/jbda.2024.020103

Layer	Key Design Decisions	Risk Mitigation Actions
	pipeline, retraining cadence, explanation layer	human-in-the-loop for consequential decisions
Strategic value	KPI / risk-index design, dashboard architecture, stakeholder reporting	Decision-rights mapping; usability testing; periodic value review
Cross-cutting governance	Consortium governance, regulatory engagement, ethics oversight	Documented governance procedures; incident-response runbooks; external assurance

Beyond technology selection, the analysis identifies three organisational competencies that distinguish successful from unsuccessful blockchain analytic deployments. The first is interdisciplinary engineering capability that bridges traditional data engineering, smart-contract development, and analytic-model engineering, because the integration of these disciplines is the critical bottleneck in most documented projects. The second is structured governance capability that articulates decision rights, escalation paths, and external accountability for the multi-party consortia within which most enterprise blockchain deployments operate. The third is sustained executive sponsorship that survives the multi-year horizon characteristic of blockchain deployment and that resists the temptation to declare premature failure during the extended period of integration learning that precedes operational value realisation.

7.3 Policy Implications

The findings also have implications for public policy. The differential maturity of the seven ecosystems suggests that regulatory clarity is a powerful determinant of adoption velocity: ecosystems in which regulators have provided clear guidance (notably finance through securities regulators and supply chain through trade authorities) have advanced more rapidly than ecosystems in which regulatory uncertainty persists (notably self-sovereign identity and governance voting). Policy-makers interested in fostering responsible blockchain analytic adoption should prioritise the development of clear, principles-based frameworks that distinguish the analytic functions that warrant regulatory attention (such as automated consequential decisions) from the underlying technical primitives (consensus and storage) that are best addressed through technical standards. Public investment in interoperability standards, regulatory sandboxes, and shared infrastructure for consortium ledgers can substantially reduce the transaction costs of cross-organisational deployment.

Privacy regulation presents a particular policy challenge. The tension between blockchain immutability and the General Data Protection Regulation's rights of rectification and erasure has occupied substantial regulatory and academic attention, but operational resolutions remain incomplete. Future regulatory guidance should clarify the conditions under which off-chain redaction, key destruction, and analogous techniques can satisfy data-protection obligations while preserving the integrity benefits of ledger anchoring. Such guidance would substantially reduce the regulatory uncertainty currently constraining blockchain adoption in healthcare, employment records, and other domains that combine high transactional volume with sensitive personal data.

8. Limitations and Future Research

Several limitations of the study constrain the generalisability of the findings and motivate productive directions for future research. First, the structured narrative review method, while appropriate for the heterogeneous and emergent character of the blockchain analytics literature, does not deliver the formal reproducibility guarantees of a strict meta-analysis. The 63 included sources represent a purposive rather than an exhaustive sample, and the synthesis depends on interpretive judgements that other reviewers might reasonably make differently. Future research that applies more formal systematic-review protocols to a narrower set of well-defined research questions would complement the broad framework developed here.

Second, the composite adoption-maturity index aggregates qualitative judgements across multiple sub-scores and reports indicative rather than precise estimates. Future work could refine this index through structured expert elicitation, bibliometric analysis of deployment-specific publications, or quantitative analysis of vendor-reported deployment counts. Such refinement would support stronger cross-ecosystem comparisons and more precise temporal tracking of adoption progress.

Third, the framework has been validated through cross-ecosystem comparison rather than through controlled empirical deployment. Future research that applies the framework to specific enterprise deployments—ideally in a design-science research mode that iterates the framework against real-world operational outcomes—would substantially strengthen its prescriptive value. Such applications should explicitly measure the four-layer interactions and the continuous risk-governance loop emphasised in the framework, providing the quantitative grounding that the present qualitative synthesis cannot deliver.

Fourth, the rapid evolution of the underlying technologies—particularly the recent emergence of large language models as analytic components and the ongoing development of zero-knowledge proof systems as privacy primitives—means that the empirical evidence base will continue to evolve quickly. The framework is designed to be robust to such evolution by focusing on the structural relationships among layers rather than on the specific technologies that occupy each layer at any given moment. Nonetheless, periodic re-validation against accumulated empirical evidence will be essential to ensure that the framework continues to track operational reality.

Beyond these limitations, three specific research directions warrant particular attention. The first is the empirical estimation of value-creation impacts across the seven mechanisms summarised in Table 2. Most published deployment reports use heterogeneous metrics that resist direct comparison; a coordinated effort to harmonise value-measurement methodology across deployments would substantially advance the field. The second is the integration of large language models and other generative-AI tools with blockchain analytics in a manner that preserves the verifiability and auditability that motivate the use of distributed ledgers in the first place. Initial work in this area (Yang et al., 2025) demonstrates the analytic potential of such integration but does not yet address the governance questions raised by deploying probabilistic generative models against immutable transactional records. The third is the development of cross-ecosystem analytic standards that would enable consistent value-comparison across blockchain deployments in finance, supply chain, healthcare, and the other ecosystems analysed in this study.

9. Conclusion

This study has developed and applied a four-layer conceptual framework for blockchain-driven business data analytics, examining the framework through the intersecting lenses of transparent transactions, risk governance, and value creation across seven digital ecosystems. The cross-ecosystem analysis reveals that the analytic value of blockchain depends less on the choice of consensus mechanism or the raw throughput of the ledger than on the integration of permissioned architectures, privacy-preserving cryptography, and intelligent oracles with enterprise governance routines. The composite adoption-maturity assessment indicates that finance and supply chain are approaching production-grade deployment, while healthcare, governance, and digital-identity applications remain at intermediate maturity and require sustained attention to regulatory engagement, privacy engineering, and stakeholder alignment. The continuous risk-governance and value-creation loop depicted in the framework provides a generalisable schema for the design of analytic systems in regulated and stakeholder-sensitive contexts beyond the specific case of blockchain.

For researchers, the study positions blockchain as the trust infrastructure of a new generation of business data analytics rather than as a self-contained protocol whose value derives from decentralisation alone. This repositioning aligns blockchain scholarship more tightly with established traditions in management analytics and decision support, and it suggests that the most productive research questions concern the integration of blockchain with analytic and organisational subsystems rather than the further refinement of consensus mechanisms whose marginal performance gains have diminishing managerial impact. For managers, the cross-ecosystem analysis suggests a sequenced investment approach that prioritises ecosystems with the deepest evidence base and clearest regulatory environment, while building the interdisciplinary engineering, structured governance, and sustained executive sponsorship capabilities that distinguish successful deployments. For policy-makers, the differential maturity of the seven ecosystems demonstrates the importance of regulatory clarity in fostering responsible adoption and motivates principles-based frameworks that distinguish analytic functions warranting regulatory attention from underlying technical primitives best addressed through technical standards.

Looking forward, the integration of blockchain with large language models, edge analytics, and quantum-resistant cryptography will introduce new analytic possibilities and new governance challenges that the framework developed here is well positioned to accommodate. The continuing evolution of digital ecosystems toward ever-greater interconnection and ever-higher stakes for the integrity of cross-organisational data flows ensures that transparent, governance-aware, value-creating analytic systems will remain a central concern for enterprises, regulators, and citizens alike. Blockchain-driven analytics offers one of the most promising technological foundations for meeting that concern, but its success will depend on the careful integration of trust infrastructure with analytic intelligence and organisational governance that the present framework has sought to articulate.

Acknowledgement

The authors gratefully acknowledge the constructive feedback provided by three anonymous reviewers, whose suggestions substantially improved the clarity and rigour of the manuscript. The

authors also thank colleagues at their respective institutions for productive discussions during the framework development phase. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Reference

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

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

Lu, Y. (2017a). Cyber physical system (CPS)-based Industry 4.0: A survey. Journal of Industrial Integration and Management, 2(3), 1750014. https://doi.org/10.1142/S2424862217500142

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

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

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. (2021a). Technological innovation and the emergence of a new interdisciplinary field: Management Analytics. Nanotechnologies in Construction, 13(3), 181-192. https://doi.org/10.15828/2075-8545-2021-13-3-181-192

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

Lu, Y. (2024). Management analytics: A bibliometric analysis. Nanotechnologies in Construction, 16(3), 257-266. https://doi.org/10.15828/2075-8545-2024-16-3-257-266

Lu, Y. (2025a). Advancing decision-making: The role of management analytics in modern business practices. Nanotechnologies in Construction, 16(5), 431-440. https://doi.org/10.15828/2075-8545-2024-16-5-431-440

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

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2024). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1-2), 2448003. https://doi.org/10.1080/17517575.2024.2448003

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473.

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

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

Yang, L., Hou, Q., Zhu, X., Lu, Y., & Xu, L. D. (2025). Potential of large language models in blockchain-based supply chain finance. Enterprise Information Systems, 19(11), 2541199. https://doi.org/10.1080/17517575.2024.2541199

Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. Systems Research and Behavioral Science, 42(4), 996-1015. https://doi.org/10.1002/sres.3050

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

Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. Journal of Management, 43(1), 39-58. https://doi.org/10.1177/0149206316678451

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. Healthcare, 7(2), 56. https://doi.org/10.3390/healthcare7020056

Akter, S., Wamba, S. F., Gunasekaran, A., Dubey, R., & Childe, S. J. (2016). How to improve firm performance using big data analytics capability and business strategy alignment? International Journal of Production Economics, 182, 113-131. https://doi.org/10.1016/j.ijpe.2016.08.018

Ali, O., Jaradat, A., Kulakli, A., & Abuhalimeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. IEEE Access, 9, 12730-12749. https://doi.org/10.1109/ACCESS.2021.3050241

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? Journal of Governance and Regulation, 6(1), 45-62. https://doi.org/10.22495/jgr_v6_i1_p5

Bai, C., & Sarkis, J. (2020). A supply chain transparency and sustainability technology appraisal model for blockchain technology. International Journal of Production Research, 58(7), 2142-2162. https://doi.org/10.1080/00207543.2019.1708989

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain technology in business and information systems research. Business & Information Systems Engineering, 59(6), 381-384. https://doi.org/10.1007/s12599-017-0505-1

Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A vademecum on blockchain technologies: When, which, and how. IEEE Communications Surveys & Tutorials, 21(4), 3796-3838. https://doi.org/10.1109/COMST.2019.2928178

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

Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. Communications of

the ACM, 63(7), 80-90. https://doi.org/10.1145/3359552

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How blockchain can impact financial services: The overview, challenges and recommendations from expert interviewees. Technological Forecasting and Social Change, 158, 120166. https://doi.org/10.1016/j.techfore.2020.120166

Chen, G., Xu, B., Lu, M., & Chen, N.-S. (2017). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1), 1. https://doi.org/10.1186/s40561-017-0050-x

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

Davenport, T., & Ronanki, R. (2018). Artificial intelligence for the real world. Harvard Business Review, 96(1), 108-116. https://doi.org/10.1109/EMR.2019.2891940

Di Vaio, A., & Varriale, L. (2020). Blockchain technology in supply chain management for sustainable performance: Evidence from the airport industry. International Journal of Information Management, 52, 102014. https://doi.org/10.1016/j.ijinfomgt.2019.09.010

Dolgui, A., & Ivanov, D. (2021). Ripple effect and supply chain disruption management: New trends and research directions. International Journal of Production Research, 59(1), 102-109. https://doi.org/10.1080/00207543.2021.1840148

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5(1), 31-37. https://doi.org/10.1109/MCC.2018.011791712

Granados, N., & Gupta, A. (2013). Transparency strategy: Competing with information in a digital world. MIS Quarterly, 37(2), 637-641. https://doi.org/10.25300/MISQ/2013/37.2.15

Greenhalgh, T., Thorne, S., & Malterud, K. (2018). Time to challenge the spurious hierarchy of systematic over narrative reviews? European Journal of Clinical Investigation, 48(6), e12931. https://doi.org/10.1111/eci.12931

Helo, P., & Hao, Y. (2019). Blockchains in operations and supply chains: A model and reference implementation. Computers & Industrial Engineering, 136, 242-251. https://doi.org/10.1016/j.cie.2019.07.023

Hofman, D., Lemieux, V. L., Joo, A., & Batista, D. A. (2019). "The margin between the edge of the world and infinite possibility": Blockchain, GDPR and information governance. Records Management Journal, 29(1/2), 240-257. https://doi.org/10.1108/RMJ-12-2018-0045

Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms. Business Horizons, 62(3), 273-281. https://doi.org/10.1016/j.bushor.2019.01.002

Hultman, J., & Axelsson, B. (2007). Towards a typology of transparency for marketing management research. Industrial Marketing Management, 36(5), 627-635.

https://doi.org/10.1016/j.indmarman.2006.04.001

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127. https://doi.org/10.1109/EMR.2017.7956601

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied Sciences, 9(9), 1736. https://doi.org/10.3390/app9091736

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

Lemieux, V. L. (2016). Trusting records: Is blockchain technology the answer? Records Management Journal, 26(2), 110-139. https://doi.org/10.1108/RMJ-12-2015-0042

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. Journal of Network and Computer Applications, 166, 102731. https://doi.org/10.1016/j.jnca.2020.102731

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

Mendling, J., Weber, I., Van Der Aalst, W., Brocke, J. V., Cabanillas, C., Daniel, F., et al. (2018). Blockchains for business process management: Challenges and opportunities. ACM Transactions on Management Information Systems, 9(1), 4. https://doi.org/10.1145/3183367

Mikalef, P., & Gupta, M. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. Information & Management, 58(3), 103434. https://doi.org/10.1016/j.im.2021.103434

Mikalef, P., Pappas, I. O., Krogstie, J., & Giannakos, M. (2018). Big data analytics capabilities: A systematic literature review and research agenda. Information Systems and e-Business Management, 16(3), 547-578. https://doi.org/10.1007/s10257-017-0362-y

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. Business Horizons, 62(1), 35-45. https://doi.org/10.1016/j.bushor.2018.08.012

Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, 117134-117151. https://doi.org/10.1109/ACCESS.2019.2936094

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80-86. https://doi.org/10.1016/j.cosrev.2018.10.002

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260. https://doi.org/10.2139/ssrn.3440802

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of blockchain technology:

Pros, cons and SWOT. Cluster Computing, 22(6), 14743-14757. https://doi.org/10.1007/s10586-018-2387-5

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

Pournader, M., Shi, Y., Seuring, S., & Koh, S. C. L. (2020). Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. International Journal of Production Research, 58(7), 2063-2081. https://doi.org/10.1080/00207543.2019.1650976

Queiroz, M. M., Telles, R., & Bonilla, S. H. (2020). Blockchain and supply chain management integration: A systematic review of the literature. Supply Chain Management: An International Journal, 25(2), 241-254. https://doi.org/10.1108/SCM-03-2018-0143

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 173-190. https://doi.org/10.1016/j.future.2018.05.046

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

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

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127-10149. https://doi.org/10.1109/ACCESS.2018.2890507

Schmidt, C. G., & Wagner, S. M. (2019). Blockchain and supply chain relations: A transaction cost theory perspective. Journal of Purchasing and Supply Management, 25(4), 100552. https://doi.org/10.1016/j.pursup.2019.100552

Sharma, P. K., Singh, S., Jeong, Y. S., & Park, J. H. (2017). DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks. IEEE Communications Magazine, 55(9), 78-85. https://doi.org/10.1109/MCOM.2017.1700041

Sun, J., Yan, J., & Zhang, K. Z. K. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation, 2(1), 26. https://doi.org/10.1186/s40854-016-0040-y

Tan, B. S., & Low, K. Y. (2019). Blockchain as the database engine in the accounting system. Australian Accounting Review, 29(2), 312-318. https://doi.org/10.1111/auar.12278

Teece, D. J. (2018). Business models and dynamic capabilities. Long Range Planning, 51(1), 40-49. https://doi.org/10.1016/j.lrp.2017.06.007

Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research

framework and a call for action. Supply Chain Management: An International Journal, 23(6), 545-559. https://doi.org/10.1108/SCM-01-2018-0029

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

Viryasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. Journal of Industrial Information Integration, 13, 32-39. https://doi.org/10.1016/j.jii.2018.07.004

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J. F., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356-365. https://doi.org/10.1016/j.jbusres.2016.08.009

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: An International Journal, 24(1), 62-84. https://doi.org/10.1108/SCM-03-2018-0148

Werbach, K. (2018). Trust, but verify: Why the blockchain needs the law. Berkeley Technology Law Journal, 33(2), 487-550. https://doi.org/10.15779/Z38H41JM9N

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

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375. https://doi.org/10.1504/IJWGS.2018.095647

Zhu, S., Song, M., Lim, M. K., Wang, J., & Zhao, J. (2022). The development of energy blockchain and its implications for China's energy sector. Resources Policy, 66, 101595. https://doi.org/10.1016/j.resourpol.2020.101595