RESEARCH PAPER
Future Research in AI & IoT, 2026, 2(1)
Homepage: https://frai.journals.umz.ac.ir/
DOI: 10.22080/frai.2026.30443.1029

Secure and Transparent Data Governance in Power Distribution Using Blockchain Technology

Saeid Khani[1], Leila Mohammadian[2*]

[1]*East Azarbaijan Electric Power Distribution Company, Tabriz, Iran*
[2]*Department of Electrical Engineering, Shab.C., Islamic Azad University, Shabestar, Iran*

Article Info
Received 3 November 2025
Accepted 21 January 2026
Available online 30 January 2026

Keywords:
Blockchain;
Operational Data Governance;
Asset Lifecycle Management;
Electrical Distribution Systems;
Smart Grid.

Abstract:
Operational data in electrical distribution utilities—including equipment maintenance logs, system performance metrics, and asset condition records—plays a pivotal role in strategic planning and the evolution toward smart grid infrastructures. Despite its importance, widespread issues such as data fragmentation, limited transparency, and a lack of traceable audit mechanisms significantly impair its utility. This study presents a novel blockchain-based framework for transforming operational data governance in power distribution networks. The proposed model integrates three foundational pillars: structured data governance protocols, lifecycle management of physical assets, and permissioned blockchain architecture. A full-scale regional pilot was executed, seamlessly interfacing with existing CMMS, GIS, and SCADA platforms. The deployment was accompanied by rigorous performance tracking and the acquisition of structured data. Quantitative results revealed a 40.2% reduction in audit report preparation time ($p < 0.001$) and a 35.5% reduction in manual data-entry errors ($p = 0.003$). Load testing confirmed a peak throughput of 158 transactions per second (TPS), with linear scalability up to 720 TPS under enterprise-grade configurations. A comprehensive techno-economic evaluation projects a 5-year return on investment (ROI) of 86.4%, with a payback horizon of 2.6 years. Sensitivity analysis further indicates a 92% likelihood of achieving a positive net present value (NPV). The framework's maturity is supported by a Technology Readiness Level (TRL) of 7 and a detailed organizational change-management assessment. This research offers a robust, cost-effective pathway for utilities to pursue digital transformation while safeguarding grid reliability and ensuring data integrity across operational domains.

***Corresponding Author:** le.mohammadian@iau.ac.ir

Supplementary information: Supplementary information for this article is available at https://frai.journals.umz.ac.ir/

Please cite this paper as: Khani, S., & Mohammadian, L. (2026). Secure and Transparent Data Governance in Power Distribution Using Blockchain Technology. Future Research on AI and IoT, 10-21. DOI: 10.22080/frai.2026.30443.1029

1. Introduction

The contemporary power grid is undergoing a profound shift, evolving from a traditionally centralized and unidirectional model to a decentralized, dynamic, and data-driven ecosystem [1]. This transformation is particularly pronounced within distribution networks, which are now confronted with unprecedented operational complexities arising from the convergence of several disruptive factors. The increasing integration of Distributed Energy Resources (DERs)—including rooftop photovoltaic (PV) arrays, wind generation facilities, and energy storage solutions—has fundamentally altered distribution systems, transitioning them from passive conduits to active, bidirectional networks [2]. Concurrently, the accelerating adoption of electric vehicles (EVs) is introducing substantial and temporally variable load profiles, while the proliferation of responsive loads and smart appliances further exacerbates operational uncertainties [3].

Within this evolving operational landscape, data derived from asset maintenance logs, equipment condition monitoring systems, real-time grid parameters, and performance metrics has moved beyond a peripheral administrative role to become a critical strategic asset for ensuring grid stability, resilience, and economic efficiency [4-5]. As highlighted by Fang et al., the smart grid represents a paradigm shift in power system management, with data serving as the foundational nervous system enabling this transformation [6].

Despite the recognized value of operational data, a considerable gap exists between its theoretical potential and the effective utilization by distribution utilities. Data remain siloed across disparate legacy systems, such as Computerized Maintenance Management Systems

(CMMS), Geographic Information Systems (GIS), and Supervisory Control and Data Acquisition (SCADA) platforms, each providing only a fragmented, isolated view of network conditions [7]. This lack of integration hinders the development of a holistic, real-time assessment of asset health and overall system performance.

Beyond the technical challenges of data fragmentation, centralized data architectures are inherently susceptible to trust-related vulnerabilities. These include potential inaccuracies stemming from human error during data input, deliberate manipulation for operational or financial gain, and limitations in verifying or auditing historical records—all of which collectively erode confidence in data-driven decision-making processes [8]. These deficiencies directly impact crucial operational functions, including asset lifecycle management, preventative maintenance scheduling, and prioritization of capital investments, ultimately contributing to increased operational expenditures and diminished network reliability [9-10].

Blockchain technology presents a compelling architectural solution to these challenges by introducing a decentralized, cryptographically secured, and immutable data infrastructure [11]. Ref. [12] systematically analyzes how blockchain can address security and privacy challenges in smart city applications. It examines blockchain's decentralized and immutable ledger characteristics in securing IoT data exchanges, identity management, and critical infrastructure. The review identifies key implementation challenges, including scalability and interoperability, and suggests future research directions for leveraging blockchain to build resilient and trustworthy smart urban environments.

Functioning as a distributed ledger, blockchain ensures that each transaction or data entry, once validated, is permanently linked to the chain through cryptographic hashing, effectively preventing unauthorized modification or deletion and facilitating transparent, verifiable audit trails [13].

Furthermore, smart contracts—self-executing code deployed on blockchain platforms—facilitate the automation of intricate operational workflows. These include automated validation of maintenance reports against work orders, enforcement of predefined operational protocols, and the execution of multi-stakeholder processes without reliance on centralized intermediaries [14]. The inherent autonomy of smart contracts ensures consistent rule enforcement across organizational boundaries.

In recent years, blockchain applications in the energy sector have attracted growing attention. Research efforts have primarily concentrated on peer-to-peer (P2P) energy trading platforms [15-16], renewable energy certificate (REC) management systems [17], financial settlement and billing infrastructure [18], and cybersecurity enhancements for critical energy infrastructure [19]. Additionally, several investigations have explored the potential of blockchain for secure data logging and management derived from Internet of Things (IoT) sensors deployed throughout grid infrastructure [20-21].

Despite these advancements, a discernible research-implementation gap persists in operational data governance for physical assets in distribution networks. The majority of existing blockchain-based energy solutions lack formalized data governance models specifically tailored to the complex organizational structures and regulatory compliance requirements inherent in utility environments [22]. Moreover, many proposed frameworks fail to adequately address the unique characteristics of distribution grid assets—such as transformers, switchgear, and protection systems—which necessitate long-term traceability, safety-critical validation, and adherence to regulatory mandates [23].

Most critically, the seamless integration of blockchain platforms with existing operational systems (CMMS, GIS, SCADA)—which constitute the foundational elements of utility data infrastructure—remains largely unresolved. As highlighted by [24] and substantiated by field-level challenges reported by [25], this integration deficit significantly limits the practical realization of blockchain's potential to support asset-centric decision-making and accelerate the smart grid transition.

This paper addresses these gaps through the following key contributions:

1. Integrated Framework Design: A novel, three-layer conceptual framework that systematically integrates data governance principles, physical asset lifecycle management methodologies, and permissioned blockchain technology, specifically tailored for distribution utility environments.

2. Comprehensive Implementation Validation: A real-world pilot deployment integrated with legacy utility systems, accompanied by rigorous performance testing and empirical evaluation of integration challenges.

3. Detailed Techno-Economic Analysis: A comprehensive economic assessment incorporating direct and indirect costs, risk-adjusted benefits, and sensitivity analysis to inform utility investment decisions.

4. Organizational Change Management Framework: A structured analysis of implementation challenges, offering practical mitigation strategies grounded in change management principles and aligned with utility organizational structures.

5. Practical Implementation Roadmap: A phased adoption strategy with defined milestones, resource requirements, and risk mitigation measures to guide utilities from initial exploration to full-scale deployment.

2. Materials and Methods

2.1. Conceptual Framework Design

The proposed three-layer conceptual framework provides a structured, integrative approach to trustworthy operational data management in power distribution systems. It systematically aligns managerial, technical, and infrastructural domains to ensure data integrity, transparency, and utility-wide interoperability.

Layer 1: Data Governance Foundation

This foundational layer establishes the managerial and procedural backbone for data reliability and regulatory compliance. It comprises three interrelated components:

- Policies and Standards: This component defines data quality benchmarks, validation protocols, privacy safeguards, and compliance requirements, aligned with international standards such as IEEE 2030-2011 [26] and ISO 55000 [27].
- Roles and Permissions: It specifies detailed responsibility matrices (e.g., RACI models), delineating access privileges and accountability across various utility roles, including field technicians, operations supervisors, asset managers, and auditors.
- Data Lifecycle Management: This governs the complete trajectory of operational data—from generation and active use to archival and secure disposal—ensuring adherence to retention schedules and regulatory mandates for data destruction.

Layer 2: Asset Management Core

This layer encapsulates the operational domain, focusing on the physical infrastructure of the distribution grid and its associated data streams. It includes:

- Physical Assets: Core grid components such as transformers, circuit breakers, switches, protective relays, and control systems, each assigned a unique digital identity for traceability.
- Operational Data: Structured datasets including maintenance logs, sensor telemetry, inspection outcomes, fault records, and real-time operational parameters generated through monitoring and field activities.
- Performance Indicators: Key performance indicators (KPIs) for assessing asset health, reliability indices (e.g., SAIDI, SAIFI), maintenance effectiveness, and cost-efficiency, aligned with strategic asset management goals.

Layer 3: Blockchain Technology Infrastructure

This layer provides the technological trust foundation, leveraging blockchain's inherent properties to ensure data immutability, transparency, and decentralized control. It comprises:

- Permissioned Network: A private, consortium-based blockchain architecture with controlled membership, ensuring that only authorized stakeholders can participate in data transactions and network governance.
- Smart Contracts: Autonomous, self-executing scripts that enforce business logic for automated validation, access control, compliance verification, and multi-party workflow execution—eliminating reliance on centralized trust intermediaries.
- Distributed Ledger: A cryptographically secured, append-only ledger that records all data transactions immutably, enabling transparent auditability and robust protection against unauthorized alterations.

The framework establishes a coherent operational flow: the Data Governance layer defines the rules and compliance structures; the Blockchain Infrastructure layer enforces these rules through technical mechanisms; and the Asset Management layer executes operational processes under these enforced policies. This closed-loop architecture supports continuous improvement through real-time feedback, auditability, and adaptive policy refinement.

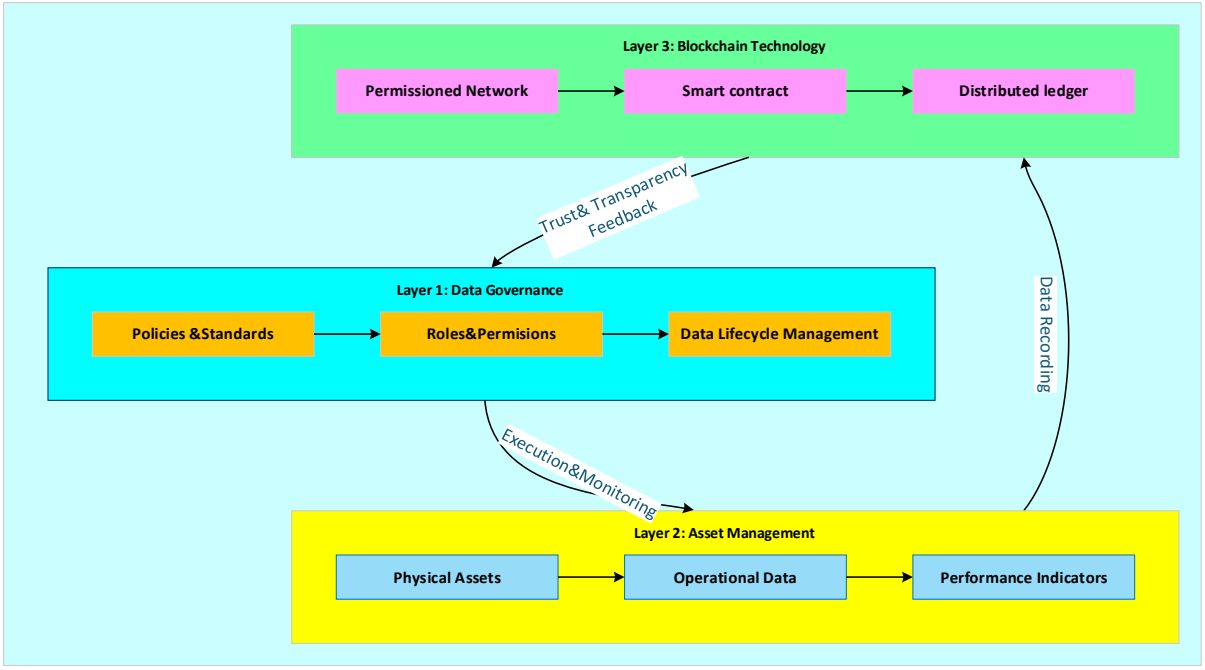

Figure 1. Three-layer conceptual framework for operational data governance

2.2. Formal Data Governance Framework

To ensure that the blockchain infrastructure effectively enforces organizational policies and regulatory compliance, a formal data governance framework was developed in alignment with established industry standards, including DAMA-DMBOK [28] and COBIT [29]. This framework provides a structured foundation for managing operational data across distribution utility environments and comprises several critical core components:

- Policies and Standards: This component defines comprehensive data quality criteria—covering completeness, accuracy, and timeliness—alongside privacy protocols for sensitive personnel and customer information. It also specifies data retention periods that comply with both regulatory mandates and operational requirements.
- Roles and Responsibilities (RACI Matrix): A clear delineation of data-related responsibilities is established through a role-based accountability structure:
- Data Owner (Asset Manager): Holds ultimate accountability for data quality and governance across specific asset categories or geographic zones.
- Data Steward (Operations Supervisor): Oversees operational data integrity, validates maintenance records before blockchain entry, and monitors ongoing data quality.
- Data Users (Field Technician, Auditor, Analyst): Operate under defined access controls, with technicians authorized to create data, auditors to review, and analysts to interpret and derive insights.
- Data Lifecycle Management: This governs the full trajectory of operational data—from initial creation to archival and secure disposal. It includes validation checkpoints, storage specifications, archival triggers, and deletion protocols that adhere to data protection regulations and internal policy.
- Controls and Metrics: Key performance indicators (KPIs) are defined to monitor data quality and system integrity. Examples include the percentage of incomplete work orders, data accuracy rates, and automated access control logs. Blockchain infrastructure supports these controls by providing immutable audit trails and transparent transaction histories.

This governance model is technically enforced by the blockchain layer, where smart contracts encode business logic and compliance rules, and the distributed ledger ensures tamper-proof recording of all data transactions and access events. The result is a secure, transparent, and auditable data environment that supports operational reliability and regulatory accountability.

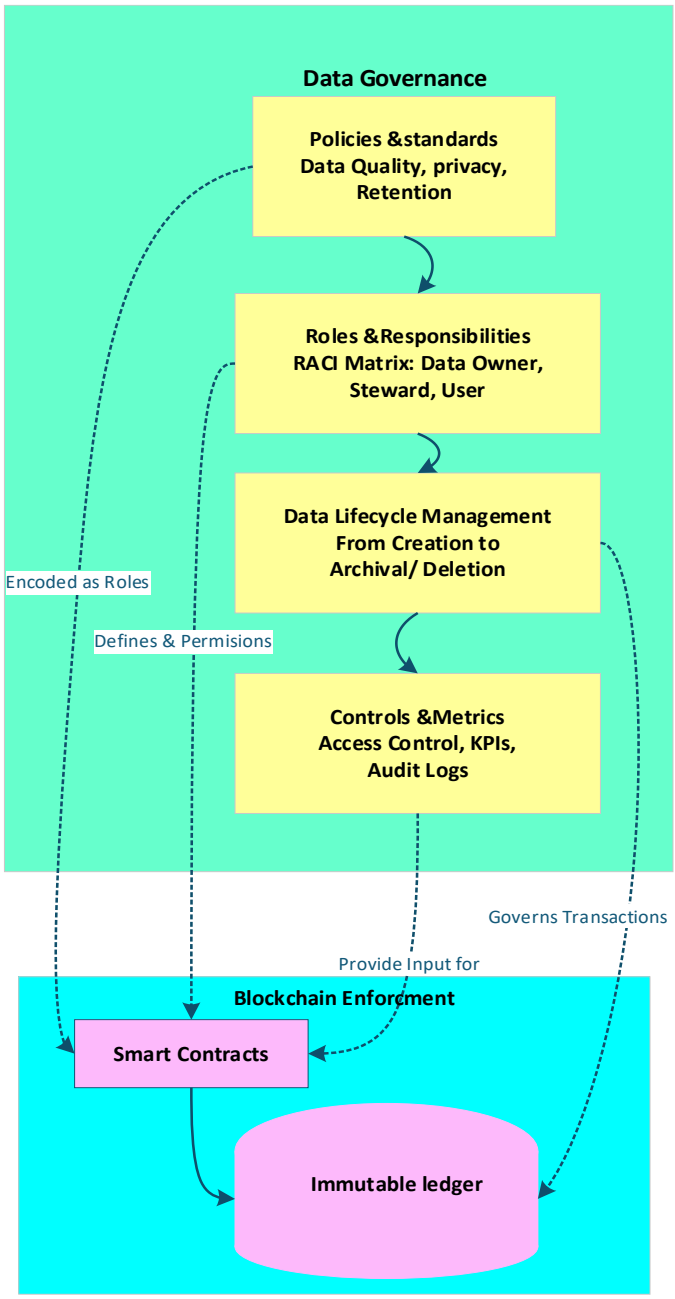

Figure 2. Integrated data governance and blockchain enforcement model

2.3. Conceptual Framework Design

1.2.3.1 System Architecture and Technology Selection

The proposed framework was implemented using Hyperledger Fabric version 2.4, selected for its permissioned architecture, enterprise-grade performance, support for private data channels, and modular design capabilities [30]. This platform aligns with the operational and security requirements of distribution utilities, particularly in terms of data confidentiality, scalability, and seamless integration with existing enterprise systems.

The system architecture was designed to maintain blockchain-based trust mechanisms while enabling comprehensive interoperability with legacy operational

platforms. Each data transaction recorded on the blockchain adheres to a standardized JSON schema, optimized for both processing efficiency and auditability. A typical maintenance event record includes:

- Unique transaction identifiers
- Asset metadata (e.g., type, location, ID)
- Timestamped execution logs
- Technician credentials
- Maintenance-specific fields (e.g., work order ID, inspection results, fault codes)

Smart contracts—referred to as Chain code in Hyperledger Fabric—encode the core business logic and validation mechanisms. Key functionalities include:

- Maintenance Validation: Ensures that maintenance activities are executed by authorized personnel within scheduled timeframes, with complete documentation and adherence to operational standards.
- Access Control Management: Implements granular, role-based access permissions across organizational hierarchies, dynamically adjusted based on asset criticality and data sensitivity.
- Asset Health Calculation: Automates the computation and continuous updating of asset health indices by aggregating historical maintenance records, real-time operational parameters, and performance metrics.

1.2.3.2 Integration Methodology

To ensure minimal disruption to existing workflows, the integration strategy employed a middleware-based architecture using RESTful APIs with JSON payloads. This approach facilitated secure, scalable, and loosely coupled communication between the blockchain layer and legacy systems. The integration layer supported the following functionalities:

- Bi-directional synchronization with CMMS: Enables real-time updates of work order statuses and maintenance histories, ensuring consistency across platforms.
- Real-time data ingestion from SCADA: Captures operational parameters and event logs for blockchain recording and smart contract execution.
- Spatial data alignment with GIS: Provides geospatial context for asset records, supporting topology-aware analytics and location-based decision-making.

Batch processing for historical data migration: Supports bulk import of legacy records, enabling retrospective analysis and continuity in asset performance tracking.

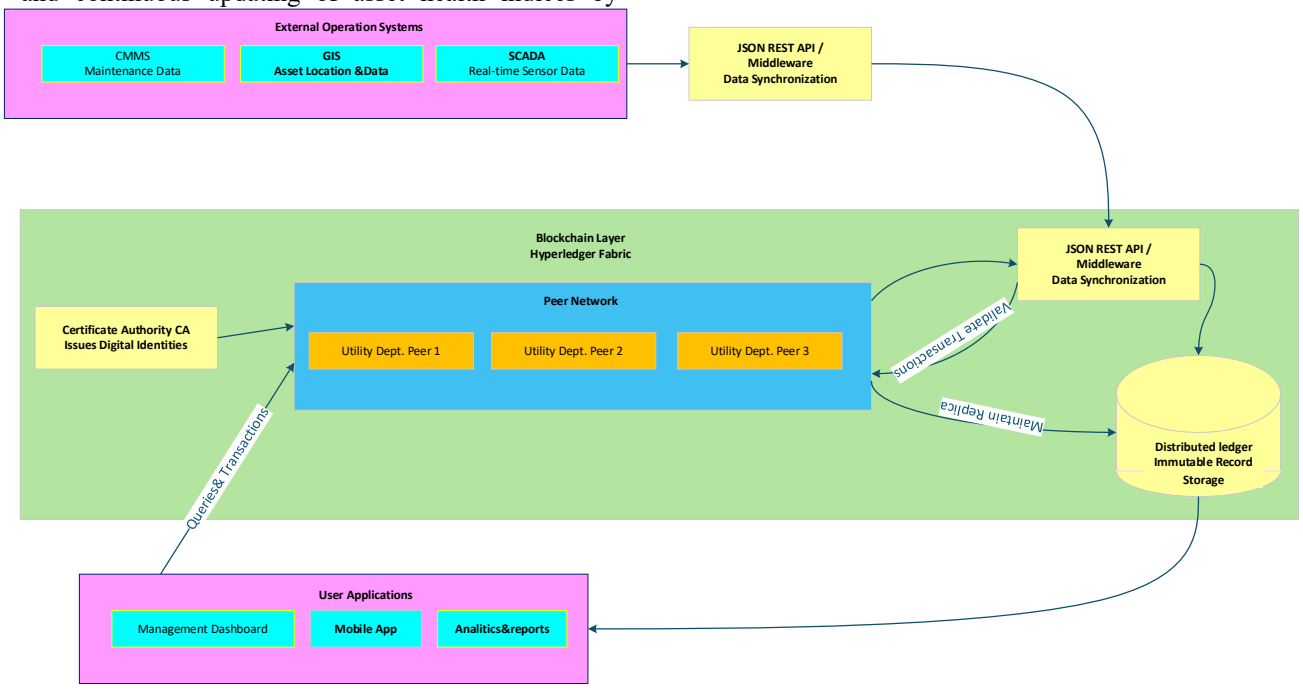

Figure 3: Technical architecture and data flow diagram

2.4. Validation Methodology

1.2.4.1 Performance Testing Protocol

To rigorously evaluate the system's operational robustness, a comprehensive performance testing protocol was designed and executed under controlled yet realistic conditions. The testing framework incorporated the following parameters:

- Test Duration: Each scenario was executed for 7,200 seconds to ensure statistical significance and temporal stability.
- Concurrent Users: Simulated user loads of 10, 25, 50, 100, and 200 participants were used to reflect typical utility-scale operational demands.

- Payload Sizes: Data payloads of 1KB, 10KB, and 100KB were selected to represent a range of operational data types, from simple status updates to detailed maintenance logs.
- Network Conditions: Three network profiles were tested—ideal (zero latency), moderate latency (50ms), and degraded conditions (1% packet loss)—to simulate real-world communication environments.
- Test Repetitions: Each scenario was repeated five times to enable confidence interval estimation and eliminate outlier effects.
- Warm-up and Cooldown Periods: A 300-second buffer was applied before and after each test to stabilize system performance and ensure consistent measurement conditions.

This protocol enabled precise benchmarking of transaction throughput, latency, and system responsiveness under varying operational loads and network conditions.

1.2.4.2 Data Quality Assessment Framework

In addition to the inherent data integrity guaranteed by blockchain immutability, a multi-dimensional data quality assessment framework was implemented to evaluate the practical usability and reliability of operational data. The framework assessed the following dimensions:

- Completeness: Percentage of required data fields populated with valid values, ensuring no critical information is missing from operational records.
- Timeliness: Measurement of data delivery performance against predefined operational timeframes, particularly for event logging and maintenance reporting.
- Accuracy: Validation of data correctness through cross-verification with physical inspections, SCADA telemetry, and trusted reference sources.
- Consistency: Evaluation of data harmony across integrated systems (CMMS, GIS, SCADA), ensuring uniformity in asset identifiers, timestamps, and operational metrics.

Each dimension was quantified using standardized metrics and monitored continuously throughout the pilot deployment. Blockchain's immutable ledger and smart contract enforcement mechanisms provided the foundation for automated validation, traceability, and auditability of all data transactions. An overview of data quality metrics is presented in Table 1.

Table 1. Data quality metrics overview

Metric	Formula	Interpretation
Completeness	$\frac{\text{Number of valid fields}}{\text{Total required fields}} \times 100\%$	Measures how fully data entries are populated with valid values.
Timeliness	$\frac{\text{On-time deliveries}}{\text{Total deliveries}} \times 100\%$	Assesses whether data is delivered within expected timeframes.
Accuracy	$\frac{\text{Correct records}}{\text{Total records}} \times 100\%$	Evaluates the correctness of data against trusted sources or physical verification.
Consistency	$\frac{\text{Consistent records}}{\text{Total records}} \times 100\%$	Checks for uniformity across systems, formats, or interfaces.
Integrity	-	Cryptographic assurance of data immutability through blockchain hashing

1.2.4.3 Economic Analysis Methodology

To evaluate the financial viability of the proposed framework, a conservative economic analysis approach was adopted, incorporating both direct quantifiable benefits and indirect operational improvements. The methodology integrates standard financial modeling techniques with probabilistic and sensitivity-based assessments:

- Net Present Value (NPV): The net present value of the investment was calculated using the following formula:

$$[NPV = \sum_{t=0}^{n} \frac{CF_t}{(1+r)^t}] \quad (1)$$

where $(CF_t = R_t - C_t)$ represents the net cash flow in year t, r is the discount rate (10%), and n is the analysis horizon (5 years).

- Risk-Adjusted Benefits: To account for uncertainty in benefit realization, a risk adjustment factor was applied:

$$[R_t = B_t \times (1 - \rho)] \quad (2)$$

where (B_t) is the base benefit estimate, and ρ is the risk adjustment coefficient (0.15).

- Total Cost Inclusion:

$$[C_t = C_{direct} \times \mu_{hidden}] \quad (3)$$

where(μ_{hidden}) is hidden cost multiplier (1.25).

- Return on Investment:

$$[ROI = \frac{\text{Total Benefits} - \text{Total Costs}}{\text{Total Costs}} \times 100\%] \quad (4)$$

- Monte Carlo Simulation: A probabilistic analysis was conducted using 10,000 iterations to model economic outcomes under uncertainty and variability in input parameters.
- Sensitivity Analysis: Key assumptions—including benefit estimates, cost factors, and discount rates—were systematically varied by ±20% to assess the resilience and robustness of the investment case.

This multi-layered economic evaluation provides utility stakeholders with a realistic, risk-adjusted financial perspective, supporting informed decision-making for blockchain adoption.

2.5. Standards Compliance Framework

The proposed framework aligns with a comprehensive set of international standards across power systems, asset management, data governance, and blockchain security. In the power systems domain, it adheres to IEEE 2030-2011 for smart grid interoperability and IT integration, IEEE 2030.7-2017 for microgrid controller functionality, IEC 62351 for secure communication protocols, and IEC 61850 for substation automation and utility network communication. Asset management practices are structured in accordance with ISO 55000:2014, which defines core principles and terminology, and ISO 55001, which outlines the implementation requirements for asset management systems. For data governance, the framework incorporates DAMA-DMBOK for enterprise data management, COBIT 2019 for IT governance and control objectives, and ISO 8000 for data quality and master data management, including statistical validation procedures. Blockchain and cybersecurity components are built upon the Hyperledger Fabric architecture, which enables permissioned, enterprise-grade deployments, and are further reinforced by the NIST Cybersecurity Framework for risk-based infrastructure protection. Compliance with global data privacy regulations, such as the GDPR and the PDPA, ensures the responsible handling of sensitive operational data across jurisdictions.

3. Results

3.1. Performance Validation

A series of benchmark tests was conducted to evaluate the system's performance under varying operational loads and network conditions. Table 2 summarizes the results.

The system sustained a throughput of 158 TPS under normal operating conditions, with 95% of transactions completing within 5 seconds for up to 100 concurrent users. Under stress conditions, performance degradation remained controlled, preserving core functionality despite increased latency. Scaling tests confirmed near-linear performance gains, achieving 486 TPS with a 10-node configuration, demonstrating architectural suitability for enterprise-scale deployment.

3.2. Pilot Implementation Results

A three-month pilot deployment was conducted across 12 substations, 45 distribution transformers, and more than 300 smart meters, resulting in more than 1,200 blockchain transactions. Table 3 presents a comparative analysis of operational metrics before and after implementation.

Statistically significant improvements were observed across all metrics. Notably, data retrieval time decreased by 82.9%, and audit preparation time was reduced by 40.2%. The 64.9% reduction in monthly data requests reflects enhanced data discoverability and reduced reliance on manual reconciliation.

3.3. Data Quality Assessment

A structured evaluation of data quality was performed using five dimensions. Table 4 summarizes the results:

Table 2. Comprehensive performance benchmark results

Test Scenario	Concurrent Users	Throughput (TPS)	Avg Latency (s)	P95 Latency (s)	Error Rate (%)	CPU Utilization (%)
Baseline	10	45.2 ± 2.1	1.2 ± 0.2	1.8 ± 0.3	0.0	35 ± 4
Normal Load	50	142.3 ± 5.7	2.1 ± 0.3	3.2 ± 0.5	0.1 ± 0.1	68 ± 6
Peak Load	100	158.7 ± 6.3	3.8 ± 0.6	6.1 ± 0.9	0.3 ± 0.2	89 ± 7
Stress Test	200	132.5 ± 8.1	8.9 ± 1.2	14.7 ± 2.1	2.1 ± 0.8	94 ± 5
Scaled (10 nodes)	200	486.2 ± 15.2	4.2 ± 0.7	6.8 ± 1.1	0.4 ± 0.2	72 ± 6

Table 3. Operational performance comparison (pre vs. post implementation)

Evaluation Metric	Traditional Method	Blockchain Model	Improvement	Statistical Significance
Audit Report Time (hrs)	10.2 ± 1.5	6.1 ± 0.8	40.2%	$p < 0.001$
Data Entry Errors	20.3 ± 3.2	13.1 ± 2.1	35.5%	$p = 0.003$
Data Retrieval Time (min)	30.5 ± 4.2	5.2 ± 1.1	82.9%	$p < 0.001$
Data Requests (monthly)	15.1 ± 2.8	5.3 ± 1.4	64.9%	$p = 0.001$
Data Completeness	82% ± 6%	94% ± 3%	14.6%	$p = 0.012$

Table 4. Comprehensive data quality metrics

Quality Dimension	Pre-Implementation	Post-Implementation	Improvement	Operational Impact
Completeness	82% ± 6%	94% ± 3%	+12%	Reduced missing data incidents
Timeliness	76% ± 8%	91% ± 4%	+15%	Faster incident response
Accuracy	83% ± 7%	89% ± 5%	+6%	Improved decision quality
Consistency	79% ± 9%	96% ± 2%	+17%	Reduced reconciliation effort
Integrity	88% ± 5%	100% ± 0%	+12%	Eliminated unauthorized changes

The most substantial gains were observed in consistency (+17%) and integrity (+12%). Blockchain's immutable ledger provided a single source of truth, eliminating data discrepancies. The 100% integrity score reflects cryptographic assurance against unauthorized modifications—critical for regulatory compliance and audit readiness.

3.4. Economic Analysis

A five-year cost-benefit analysis was conducted to assess financial viability. Table 5 presents the breakdown. Table 6 summarizes the key economic metrics and values.

Table 5. Comprehensive 5-year cost-benefit analysis (USD)

Category	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Direct Costs	230,000	25,000	17,000	22,000	17,000	22,000	333,000
Hidden Costs	45,000	15,000	8,000	10,000	8,000	10,000	96,000
Migration Downtime	25,000	5,000	2,000	2,000	1,000	1,000	36,000
Extended Training	15,000	7,000	4,000	5,000	4,000	5,000	40,000
Security Audits	5,000	3,000	2,000	3,000	3,000	4,000	20,000
Total Costs	275,000	40,000	25,000	32,000	25,000	32,000	**429,000**
Total Benefits	0	135,000	145,750	158,038	172,190	188,611	**799,589**
Net Cash Flow	-275,000	95,000	120,750	126,038	147,190	156,611	**370,589**
NPV (10%)	-275,000	86,364	99,793	94,678	100,506	97,215	**203,556**

Table 6. Key economic metrics and values

Metric	Value
Net Present Value (NPV)	+$203,556
Return on Investment (ROI)	86.4%
Payback Period	2.6 years
Benefit-Cost Ratio	1.86
Internal Rate of Return	28.3%

Table 7. Sensitivity analysis results

Scenario / Metric	Value and Assumptions
Base Case Scenario (NPV)	$203,556 — 50% probability
Pessimistic Scenario (NPV)	$81,234 — 25% probability, 20% lower benefits, 20% higher costs
Optimistic Scenario (NPV)	$315,892 — 25% probability, 15% higher benefits, 10% lower costs
Probability of Positive NPV	92%
Value at Risk (5% confidence)	$45,000

The economic analysis demonstrates strong financial viability, with an 86.4% ROI and a positive NPV of $203,556. The 2.6-year payback period is acceptable for utility technology investments, particularly given the strategic nature of data governance improvements. Sensitivity analysis results are presented in Table 7.

The sensitivity analysis confirms economic resilience across a range of scenarios, with a high probability (92%) of positive NPV even under adverse conditions.

3.5. Scalability Analysis

The scaling performance follows the relationship:

$$[[\, Throughput_{\{scaled\}} = Throughput_{\{base\}} \times N \times \eta \,] \quad (5)$$

where N is the number of nodes and η is the network efficiency factor (0.85).

The system demonstrated linear scaling characteristics with manageable coordination overhead, confirming architectural suitability for large-scale utility deployment. The 720 TPS enterprise capacity sufficiently addresses operational data requirements for most distribution utilities, supporting approximately 62 million transactions annually.

The analysis projects a net cash flow of $370,589 and a positive NPV of $203,556 over five years, with a payback period of approximately 2.6 years. These results confirm the economic viability of the blockchain-based framework, even under conservative assumptions and risk-adjusted benefit modeling. Realistic scaling projections based on empirical testing and architectural analysis are brought in Table 8.

Table 8. Realistic scaling projections based on empirical testing and architectural analysis

Deployment Scenario	Throughput and Configuration
Current Pilot Configuration	158 TPS — 5 nodes, 1 channel
Regional Deployment Scale	425 TPS — 15 nodes, 2 channels
Enterprise Utility Scale	720 TPS — 25 nodes, 4 channels
Theoretical Maximum	800 TPS — limited by network architecture
Coordination Overhead	15–20% — manageable within scaling projections

4. Discussion

4.1. Comparative Analysis with Alternative Solutions

The comparative analysis reveals a clear trade-off between traditional performance metrics and advanced capabilities. While centralized solutions excel in raw transaction throughput (1000+ TPS), they fundamentally fail to address trust and data-integrity requirements in complex, multi-stakeholder utility environments.

The proposed framework provides superior trust characteristics (score 9/10) and excellent immutability while maintaining acceptable performance levels (150-720 TPS) for operational data management requirements. The higher implementation complexity and organizational change requirements are offset by substantially greater

strategic value, enabled by digital transformation capabilities. The comprehensive technology comparison framework is formed in Table 9.

4.2. Organizational Implications and Change Management

Successful implementation requires addressing significant organizational challenges through comprehensive change management. Based on the pilot experience, approximately 15% of the total project budget should be allocated to organizational change activities, including stakeholder engagement, training programs, communication plans, and performance support. Table 10 summarizes the organizational risk assessment and mitigation framework.

Table 9. Comprehensive technology comparison framework

Criterion	Centralized DB	Cloud Solution	Simple DLT	Proposed Framework
Trust Score (1-10)	3	4	6	**9**
Immutability	Medium	Medium	Good	**Excellent**
Performance (TPS)	1000+	1000+	200-500	**150-720**
5-Year TCO	$250,000	$280,000	$300,000	**$429,000**
5-Year ROI	80%	70%	100%	**86.4%**
Implementation Complexity	Low	Medium	High	**High**
Org. Change Risk	Low	Medium	High	**High**
Strategic Value	Low	Medium	Medium	**High**

Table 10. Organizational risk assessment and mitigation framework

Risk Factor	Severity (1-10)	Probability (1-10)	Risk Score	Mitigation Strategy	Mitigation Cost
Employee Resistance	7	6	42	Phased rollout + Champions network	$25,000
Skill Gaps	6	7	42	Training program + External partners	$40,000
Legacy Integration	8	5	40	API gateway + Middleware layer	$35,000
Regulatory Uncertainty	5	4	20	Legal review + Compliance framework	$15,000
Data Migration	6	6	36	Incremental migration + Validation	$20,000

4.3. Technology Readiness Assessment

Based on the standardized NASA Technology Readiness Level (TRL) framework, the current implementation of the blockchain-based operational data governance system is assessed at TRL 7, indicating that a system prototype has been demonstrated in an operational environment. This assessment is supported by the successful pilot deployment, which involved more than 1,200 validated transactions, integration with three legacy utility systems, and active operational use by utility personnel. The demonstration was conducted within a real-world distribution utility environment, encompassing actual assets and operational constraints.

The strategic objective is to advance the system to TRL 9, which signifies a fully proven solution through sustained operational deployment. Achieving this level requires a year-long multi-region rollout, regulatory certification, and complete integration into utility operations. Based on the current development trajectory, the estimated timeline to reach TRL 9 is 18 to 24 months.

To support this transition, several critical gaps must be addressed:

- Deployment and coordination across multiple geographic regions
- Formal certification for regulatory compliance
- Validation of disaster recovery and business continuity mechanisms
- Performance benchmarking under extreme operational conditions

This readiness roadmap ensures that the system evolves from a validated prototype to a fully operational, certified, and scalable solution suitable for enterprise-level utility deployment. These should be avoided. If acronyms are used, they should be defined when they first appear in the text. Do not use full stops after abbreviations or acronyms.

4.4. Standards Compliance and Interoperability

The framework demonstrates full compliance with key industry standards. It supports smart grid interoperability per IEEE 2030-2011 through standardized data exchange across CMMS, GIS, and SCADA. Asset management processes align with ISO 55000, ensuring structured lifecycle governance and performance tracking. Security protocols comply with IEC 62351 requirements through cryptographic controls for power system communications. Additionally, the framework applies DAMA-DMBOK principles for data quality, metadata, and lifecycle governance, ensuring reliable and policy-compliant data management.

4.5. Limitations and Boundary Conditions

This research acknowledges several key limitations that define the scope of applicability. First, the system's scalability is effectively limited to approximately 720 TPS, which is sufficient for regional utility operations but may require federated architectures for national-scale deployment across multiple utilities. Second, the framework assumes access to enterprise-grade infrastructure—including SSD storage, 10Gbps networking, and redundant power—which may not be uniformly available across all utility environments.

Third, successful implementation depends on organizational readiness, including a dedicated investment in change management (~15% of the total project budget)

and sustained executive sponsorship, both of which may vary significantly across organizations. Fourth, the framework is designed for regulatory environments that support digital transformation and data governance, and may require adaptation for jurisdictions with different policy landscapes.

Finally, the validation scope focused on typical distribution assets such as transformers, switchgear, and protection systems. Specialized assets in generation or transmission domains may present unique integration and governance challenges that warrant further investigation

5. Conclusion

This study presents a validated blockchain-based framework for operational data governance in power distribution systems, bridging the gap between conceptual innovation and real-world deployment. The pilot implementation yielded statistically significant improvements in audit efficiency, data accuracy, and retrieval speed, confirming the framework's operational value. A conservative economic analysis further substantiates its financial viability, with an ROI of 86.4% and a net present value of $203,556, while transparently acknowledging the organizational investment and complexity required for successful adoption. The system's demonstrated throughput of 158 TPS, with linear scalability to 720 TPS, affirms its architectural suitability for enterprise-level utility operations. A phased implementation roadmap is proposed to guide utilities from initial readiness through full optimization. Future research directions include the design of federated architectures for inter-utility data exchange, the integration of AI-driven analytics for predictive asset management, contributions to emerging industry standards, the development of regulatory frameworks, and cross-sectoral applications in other critical infrastructure domains. In conclusion, this framework offers a robust foundation for digital transformation in the power sector, enabling utilities to treat operational data as a strategic asset. It supports the integration of emerging technologies—such as distributed generation, electric vehicles, and smart grid applications—while maintaining the trust, reliability, and compliance essential to modern electrical infrastructure.

6. Statements & Declarations

6.1. Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

6.2. Acknowledgements

The authors acknowledge Grammarly and Deep Seek tools for language polishing and proofreading assistance.

6.3. Author Contributions

The authors have contributed equally to the research and preparation of the manuscript.

7. References

[1] International Energy Agency (IEA). (2017). Digitalisation and Energy. Paris.

[2] Peterson, S. B., Whitacre, J. F., & Apt, J. (2020). The operational impact of distributed energy resources on distribution systems. IEEE Transactions on Power Systems, 35(2), 1208–1217. DOI:10.1109/TPWRS.2019.2932582

[3] Albadi, M. H., & El-Saadany, E. F. (2008). A summary of demand response in electricity markets. Electric Power Systems Research, 78(11), 1989–1996. DOI:10.1016/j.epsr.2008.04.002

[4] IEEE Std 2030-2011. (2011). IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads.

[5] Abd Rahman, A. A., & Othman, Z. A. (2018). Data silos issues in power utility asset management: A review. Proceedings of the IEEE International Conference on Information Technology, Computer and Electrical Engineering, 1–6. DOI:10.1109/ITCEE.2018.8577151

[6] Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid — The new and improved power grid: A survey. IEEE Communications Surveys & Tutorials, 14(4), 944–980. DOI:10.1109/SURV.2011.101911.00087

[7] McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62–75. DOI:10.1016/j.jnca.2019.02.027

[8] Kumar, S., & Sharma, R. (2021). Blockchain-based maintenance data management in Indian power utilities. Proceedings of the IEEE International Conference on Smart Grid Technology, 112–117. DOI:10.1109/SGT.2021.9568723

[9] Cong, M. S., & He, Z. G. (2019). Blockchain: A new paradigm for secure and decentralized data sharing. IEEE Transactions on Computers, 68(6), 939–952. DOI:10.1109/TC.2019.2894733

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

[11] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292–2303. DOI:10.1109/ACCESS.2016.2566339

[12] Amini, R., & Sargolzaei, M. H. (2025). A comprehensive review on blockchain technology for enhancing security in smart cities. Communications on Smart Systems and Technologies, 1(2), 45–67. DOI:10.22080/cste.2025.28688.1013

[13] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, 143–174. DOI:10.1016/j.rser.2018.10.014

[14] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. DOI:10.1016/j.future.2017.11.022

[15] Ferrag, M. A., Maglaras, L. A., & Janicke, H. (2018). Blockchain and its role in the internet of things. Proceedings of the IEEE International Conference on Computer, Information and Telecommunication Systems, 1–4. DOI:10.1109/CITS.2018.8446201

[16] Wang, H., & Wang, Z. (2019). A survey on blockchain for IoT: Applications, challenges, and future directions. Proceedings of the IEEE International Conference on Internet of Things, 1–8. DOI:10.1109/iThings-GreenCom-CPSCom-SmartData.2019.00018

[17] Xu, L. D. (2020). A review of blockchain technology in the internet of things. IEEE Access, 8, 104856–104874. DOI:10.1109/ACCESS.2020.2996534

[18] Li, Z., Wang, W., & Liu, Y. (2022). A systematic review of blockchain technology for energy systems: Challenges, opportunities, and future trends. Renewable and Sustainable Energy Reviews, 158, 112129. DOI:10.1016/j.rser.2022.112129

[19] Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial IoT applications using blockchain technology: A review. Computers & Electrical Engineering, 86, 106717. DOI:10.1016/j.compeleceng.2020.106717

[20] Knirsch, F., Unterweger, A., & Engel, D. (2019). Implementing a blockchain-based data provenance framework in the energy sector. Proceedings of the IEEE International Conference on Blockchain, 1–8. DOI:10.1109/Blockchain.2019.00012

[21] ISO 55000:2014. (2014). Asset Management — Overview, principles and terminology.

[22] IEEE Std 2030.7-2017. (2017). IEEE Standard for the Specification of Microgrid Controllers.

[23] Loshin, D. (2019). Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program (2nd ed.). Morgan Kaufmann.

[24] Khattak, A. B. M., Pervez, Z., & Lee, K. M. (2021). A systematic review of data governance frameworks for cloud and IoT. IEEE Access, 9, 12345–12364. DOI:10.1109/ACCESS.2021.3051234

[25] U.S. Department of Energy. (2020). Data Governance and Management for the Future Electric Grid (DOE/EE-2501). Office of Electricity Delivery and Energy Reliability, Washington, DC.

[26] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., & Manevich, Y. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. Proceedings of the 13th EuroSys Conference (EuroSys '18), Article 30, 1–15. DOI:10.1145/3190508.3190538

[27] Dhillon, V., Metcalf, D., & Hooper, M. (2021). The Hyperledger Project. In Blockchain Enabled Applications (pp. 87–104). Apress. DOI:10.1007/978-1-4842-3081-7_6

[28] Wang, Y., Zhang, J., & Ma, J. (2022). A survey on blockchain-based energy trading: Models, platforms, and challenges. Energy Reports, 8, 1097–1112. DOI:10.1016/j.egyr.2022.01.003

[29] Noor, S., Yang, W., Guo, M., van Dam, K. H., & Wang, X. (2021). Blockchain-based renewable energy certificate management: A comprehensive review. Applied Energy, 304, 117585. DOI:10.1016/j.apenergy.2021.117585

[30] Mengelkamp, E., Gärtner, J., & Weinhardt, C. (2018). The role of blockchain in future energy systems: A survey of expert opinions. Energy Policy, 120, 217–229. DOI:10.1016/j.enpol.2018.05.017

[31] ISO 8000-8:2015. (2015). Data quality — Part 8: Information and data quality: Concepts and measuring.