IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46AI/2025/4643025/
Vol. 2025 (34), Article ID 4643025

"Data Trust Architecture: ISO Standards and the Evolution of the Data Governance 3.0 Model in Blockchain Ecosystems" *

Malgorzata MICHNIEWICZ

Military University of Technology, Warsaw, Poland

Correspondence should be addressed to: Malgorzata MICHNIEWICZ, malgorzata@michniewicz.org

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

The rapid growth of distributed ledger technologies (DLT) and new regulatory obligations (GDPR, DORA, NIS2, AI Act) are forcing organisations to rethink how they govern data as a strategic and auditable asset. However, existing data-governance models and standards only partially address trust, accountability and interoperability in decentralised ecosystems. This paper proposes the concept of Data Governance 3.0 and a corresponding Data Trust Architecture (DTA) that position blockchain as a technical trust layer for data-driven and AI-enabled systems.
The study applies an interpretive review of international standards (ISO/IEC 8000, 27001, 38505, 22739, 23245–23258, 23635, 6277; IEEE 2418.x, 2145, 3447; NIST, ISACA) and academic and professional literature from 2016–2024. On this basis, it traces the evolution from centralised control (Data Governance 1.0), through federated data-product models (2.0, Data Mesh), to decentralised trust-based governance (3.0). The paper synthesises these sources into a four-layer DTA model (governance and policy; identity and access; integrity and provenance; interoperability and automation) with clearly defined organisational roles.

The findings show that Data Governance 3.0 enables data to function as a self-verifiable trust asset, providing cryptographic evidence of integrity, provenance and policy compliance across organisational boundaries. The proposed DTA provides a reference framework for designing accountable and interoperable data ecosystems, integrating blockchain, AI, Data Mesh and Compliance-as-Code. The paper concludes with research directions for formalising data-trust metrics and cross-chain interoperability in future Data Trust 4.0 architectures.

Keywords: data governance, blockchain, Data Trust Architecture, data accountability

Introduction

The importance of data trust – data quality and data value

Modern organisations operate in an environment where data has become one of the key assets determining competitive advantage. However, the value of data is revealed only when it is reliable, consistent, and accountable. Data trust therefore becomes the foundation of modern information governance — in both its technological and organisational dimensions.

According to ISO 8000-2:2022 – Data Quality – Vocabulary, data quality is defined as "the degree to which data satisfies the requirements of its intended use." This means that high-quality data are not only syntactically and semantically correct but also transparent and verifiable in terms of origin, integrity, and context of use. In this sense, data quality becomes the basis of trust — enabling source identification, reliability assessment, and accountability for data-driven decisions.

Cite this Article as: Malgorzata MICHNIEWICZ, Vol. 2025 (34) "Data Trust Architecture: ISO Standards and the Evolution of the Data Governance 3.0 Model in Blockchain Ecosystems " Communications of International Proceedings, Vol. 2025 (34), Article ID 4643025, https://doi.org/10.5171/2025.4643025

Data quality is not a static state but a continuous process of confirming authenticity, integrity, and responsibility for data. Mechanisms of auditability and immutability, described in ISO/TC 307 (Blockchain and Distributed Ledger Technologies) and NIST IR 8202, play a critical role in this process. Distributed ledger technologies enable the creation of "proofs of integrity" (hashes) and "data lineage chains", which make it possible to verify data reliability independently of data ownership.

In this context, data trust represents a new dimension of data quality, encompassing four key pillars:

- integrity – ensuring that data has not been modified in an unauthorized manner;
- provenance – the ability to trace the origin and transformations of data throughout its lifecycle;
- accountability – assigning responsibility for data processing and sharing;
- transparency – enabling independent verification of data quality and compliance with organisational policies.

According to ISO 22739:2024 (sections 3.23, 3.10, 3.47), distributed ledger technologies (DLT) are defined as "a distributed ledger containing confirmed blocks, in which information is recorded in an append-only, sequential manner using cryptographic hash links." Their key properties — immutability, auditability, and consensus — provide the technical foundations of data trust and enable the verification of authenticity without the need for a central intermediary.

Within the ISO Technical Committee TC 307, standards are currently being developed to define a common interoperability language for blockchain technologies, enabling the integration of data systems across multi-chain and inter-organisational models (see Table 1). The ISACA Blockchain Framework, in turn, indicates that data trust can be measured and audited through objective criteria such as ledger integrity, data quality, and compliance with consensus mechanisms and organisational policies.

Data trust thus bridges technological, organisational, and normative dimensions, encompassing both quality control and compliance with ethical principles and legal regulations (GDPR, DORA, NIS2, AI Act). Modern Data Governance 3.0 frameworks assume that data becomes a self-verifiable asset, capable of demonstrating its own integrity and value. In this paradigm, blockchain functions as the trust layer, while ISO standards provide a shared language for auditability and interoperability.

From Information Management to Data Value Management

Traditional information management focused primarily on the collection and protection of data, treating it as a supporting resource for business processes. In the Data Governance 1.0 model, data were viewed as a byproduct of operational activity rather than as an asset of measurable value.

With the advancement of predictive analytics, artificial intelligence, and the data economy, the focus has shifted from information management to data value management (DVM). This shift involves not only ensuring data quality and security but also managing the economic, ethical, and trust-related aspects of data use.

The ISO/IEC 38505-1:2017 standard emphasizes that data should be treated as a governance asset, whose value can be increased through quality control, accountability, and alignment with organisational objectives. This view is consistent with multidimensional understanding of value in blockchain ecosystems, which encompasses technological, economic and governance dimensions (Ciupa,2020). In this sense, data become a "product" (Data as a Product) characterized by:

- a data owner;
- defined metadata and quality levels (SLA);
- a clearly defined lifecycle and business purpose.

In the Data Governance 3.0 model, the value of data no longer derives solely from its volume but from the level of trust it commands. Blockchain and other DLT technologies provide the technical foundation of this trust — recording proofs of authenticity, protecting integrity, and enabling auditability of changes. Combined with the concept of Compliance-as-Code, data become a self-regulating resource that automatically meets quality, compliance, and ethical requirements throughout its flow within the organisation.

As a result, a new paradigm emerges: from Data Management to Data Trust Management, where data are not only managed but also attest to their own quality, provenance, and value.

Research gap, objective and scope of the study

Although there is a rich body of literature on data governance frameworks (e.g. COBIT, DAMA-DMBOK, Data Mesh) and a rapidly growing portfolio of standards for blockchain and DLT, existing approaches typically address these areas in isolation. Data governance models rarely integrate blockchain-based trust mechanisms at the architectural level, while technical standards for DLT tend to focus on protocols and security rather than on their role as a trust layer for data ecosystems. As a result, there is a lack of an integrated model that connects data governance, data quality and accountability with blockchain-based trust and with concrete ISO/IEC, IEEE, ISACA and NIST standards.

The purpose of this paper is to address this gap by presenting the evolution of data management from centralized control models (Data Governance 1.0), through federated approaches (Data Governance 2.0, Data Mesh), to modern solutions based on accountability, trust and decentralization (Data Governance 3.0). The article analyses how standards developed by ISO/IEC, IEEE, ISACA and NIST together form the foundation of the emerging concept of Data Trust Architecture (DTA), integrating the data governance layer with the trust layer (blockchain and DLT).

The paper makes three main contributions:

1. It conceptualizes Data Governance 3.0 as a trust-oriented evolution of previous governance models, explicitly linking data value to verifiable trust.
2. It synthesizes international standards into a four-layer Data Trust Architecture that connects governance and policy, identity and access, integrity and provenance, as well as interoperability and automation.
3. It proposes an interpretive framework for designing trusted, accountable and interoperable data ecosystems in which blockchain acts as a technical trust layer for AI, Data Mesh and Compliance-as-Code environments.

The scope of the study covers standards and literature related to data governance, blockchain/DLT, data quality, audit and regulatory compliance, with a specific focus on the period 2016–2024, when Data Governance 2.0 and 3.0 concepts and DLT standards matured.

Nr	**Number**	**Title**	**Year of publication**	Kind of standard
1	ISO/TR 23455:2019	*Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and DLT systems*	2019	TR
2	ISO/PAS 23263:2019	*Blockchain and distributed ledger technologies — Functional categories for service and platform*	2019	PAS
3	ISO/TR 23576:2020	*Blockchain and distributed ledger technologies — Security management of digital asset custodians*	2020	TR
4	ISO/TR 23244:2020	*Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations*	2020	TR
5	ISO 22739:2024	*Blockchain and distributed ledger technologies — Vocabulary*	2024	ISO
6	ISO/TR 23245:2021	*Blockchain and distributed ledger technologies — Taxonomy and classification of DLT-based payment systems*	2021	TR

7	ISO/TR 23246:2021	*Blockchain and distributed ledger technologies — Overview of existing DLT systems for identity management*	2021	TR
8	ISO 23257:2022	*Blockchain and distributed ledger technologies — Reference architecture*	2022	ISO
9	ISO 23258:2022	*Blockchain and distributed ledger technologies — Taxonomy and ontology for smart contracts*	2022	ISO
10	ISO/TS 23635:2022	*Blockchain and distributed ledger technologies — Guidelines for governance*	2022	TS
11	ISO/TR 6277:2024	*Blockchain and distributed ledger technologies — Data flow models for blockchain and DLT use cases*	2024	TR

PAS — Publicly Available Specification, TS — Technical Specification, TR — Technical Report
Table 1:Published standards by ISO/TC 307

Currently, the Technical Committee ISO/TC 307 is developing more than 20 standards and projects related to blockchain and DLT security.

Evolution of data governance

The evolution of data governance reflects the changing needs of organisations and the digital society — from simple information-control models, through federated data-flow management, to trust architectures based on accountability and decentralization.

Data governance has ceased to be merely an operational IT function; it has become a system of trust and value, in which data are not only an asset but also a carrier of credibility.

Data Governance 1.0 – centralization and control

The first data-governance models, developed in the 1990s and early 2000s, focused on centralization, quality control, and data security. They were built on corporate standards and information-management methodologies such as COBIT 4 (ISACA, 2005), DAMA-DMBOK 1.0 (2009), and Master Data Management (MDM) systems.

The goal was to establish a single, consistent "organisational truth" (a single source of truth), managed by a central team of data stewards.

In this model, data were seen mainly as a by-product of operational activity. Managing them meant defining rules for access, quality, and compliance — not assessing their potential business value. Data-quality standards such as ISO/IEC 25012:2008 – Data Quality Model and early editions of ISO/IEC 8000 defined metrics of accuracy, completeness, and consistency, but did not yet address trust, accountability, or ethical context.

Characteristic features of Data Governance 1.0:

• strong centralization of responsibilities and decisions;

• focus on control and compliance (compliance-driven);

• separation of the data layer from business strategy;

• lack of accountability mechanisms and dynamic quality verification.

This model proved effective in stable corporate structures but insufficient in the era of distributed data and real-time analytics.

Data Governance 2.0 – federation, data mesh, and automation

Around 2015, a turning point occurred — the rapid growth of data volumes and cloud services drove a shift from centralization to federation and shared accountability.

The concept of Data Governance 2.0 was first broadly described in the DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK 2, 2017) and further developed by Zhamak Dehghani (2022) as the Data Mesh paradigm.

In this approach, data are treated as a product (Data as a Product), and responsibility for their quality and usefulness is distributed across business domains. New notions emerged, such as:

• data product owner – responsible for data value and availability;
• data marketplace – a repository of datasets with measurable quality and service-level agreements (SLA);
• automation of governance – implementation of quality and compliance rules as code (*Compliance-as-Code*).

During this period, data-audit frameworks were also developed, combining IT-governance, data-quality, and compliance perspectives, as seen in COBIT 5 for Information Security and COBIT for Assurance (ISACA, 2013-2015), together with ISO standards on corporate data governance — including ISO 8000 (Data Quality Series), the ISO 27000 family on information security (notably ISO/IEC 27040:2015 Storage security), and ISO/IEC 38505-1:2017 Governance of IT for the organisation, which for the first time stated that data should be treated as measurable assets.

The Data Governance 2.0 model was the first to integrate technology, value, and process, yet it still lacked embedded trust and auditability guarantees.

Data Governance 3.0 – accountability, trust, and decentralization

The current phase, referred to as Data Governance 3.0, has been evolving since around 2022 in response to the need for trusted, interoperable data ecosystems capable of self-verifying integrity, provenance, and compliance. This model addresses the growing complexity of data, the automation of decision-making in AI, and new regulatory demands (AI Act, DORA, NIS2, MiCA, CRA).

According to ISO/TC 307 standards — including ISO 22739:2024 (Blockchain and DLT Vocabulary), ISO/TS 23258:2021 (Taxonomy and Ontology), ISO 23257:2022 (Reference Architecture), and the forthcoming ISO 20435 (Auditing Guidelines) — blockchain technology serves as a Trust Layer in modern data architectures. This enables a transition from *"control & access"* to *"trust & accountability"*, where data become self-verifiable, and every operation is recorded and auditable.

Key features of Data Governance 3.0:

• decentralization and interoperability – governance distributed among entities and domains;
• accountability – integrity evidence, auditability, and compliance with policies;
• trust – cryptographically ensured and validated through ISO/ISACA standards;
• Compliance-as-Code – automated enforcement of quality and security policies via smart contracts;
• ethics and transparency – alignment with the FAIR principles (Findable, Accessible, Interoperable, Reusable) and the NIST AI Risk Management Framework (2023).

In this view, data are no longer merely a resource — they become a trust asset, capable of proving their own quality and value. In recent ISO definitions, an *asset* is understood as anything that holds value for stakeholders. This model forms the foundation of the Data Trust Architecture 3.0, which unifies ISO frameworks, blockchain, and audit mechanisms into a coherent ecosystem of data accountability.

Standards in the context of data trust

As the importance of data continues to grow, a key challenge has become ensuring the consistency, auditability, and interoperability of data ecosystems.

International standards form the foundation of this process — they not only unify concepts and processes but also establish trust frameworks that enable cooperation among systems in inter-organisational and decentralized models.

Organisations such as ISO (International Organisation for Standardization), IEEE, ISACA, and NIST (National Institute of Standards and Technology) play complementary roles in developing standards for data quality, security, accountability, and compliance.

The most important standards and guidelines in the area of Data Trust can be grouped into four interrelated domains:

1. Governance and Quality – standards defining data governance, value, and accountability;
2. Identity and Provenance – standards addressing data identity, lineage, and origin;
3. Integrity and Audit – standards ensuring integrity, auditability, and regulatory compliance;
4. Interoperability and Automation – standards enabling data exchange and the enforcement of rules.

Governance and quality – ISO/IEC 8000, 38505 and 23635

The foundation of the Data Trust concept lies in the ISO/IEC 8000 family of standards, which define the frameworks for data quality and data management.
The ISO 8000:2022 series describes processes for data quality assessment, including methods for validation and certification of data sources. When combined with the ISO/IEC 38505 series (*Governance of Data*), this forms a structural model of accountability — specifying *who* is responsible, *for what*, and *to what extent* throughout the data lifecycle.

A new complement to this framework is the emerging ISO/TS 23635:2022 – Guidelines for Governance, developed under ISO/TC 307. This document extends the perspective from traditional data management to ecosystem-level trust governance, integrating quality and ethics policies with the technological frameworks of Distributed Ledger Technologies (DLT) and AI governance.

Identity and provenance – ISO 23258, 22739 and W3C DIDs

Trust in data requires a verifiable identity of both users and the data themselves.
The standards ISO/TS 23258:2021 – "Taxonomy and Ontology for Smart Contracts" and ISO 22739:2024 – "Vocabulary for Blockchain and Distributed Ledger Technologies (DLT)" define the core concepts of interoperability, provenance, and data accountability in distributed systems. Together with the W3C Decentralized Identifiers (DIDs, 2022) recommendation, they form the foundation for decentralized data provenance, enabling the unambiguous identification of data sources, owners, and transformations within Data Mesh and Data Trust Architecture 3.0 frameworks.

For example, these standards enable the implementation of:
- Trusted Data Lineage – cryptographically verifiable tracking of data flows and modifications;
- Verifiable Credentials – confirmation of data authenticity and origin without intermediaries;
- Federated Trust Domains – interoperable trust frameworks between organisations.

Integrity and audit – ISO/CD TS 23353.2, ISACA, NIST

Trust in data requires measurable accountability and auditability.
The draft standard ISO/CD TS 23353-2 – "Auditing Guidelines for Blockchain and Distributed Ledger

Technologies (DLT)" is being developed to define principles for auditing the integrity of data recorded in distributed systems. The document will provide methods for assessing blockchain quality, identifying consensus risks, and evaluating compliance with data policies.

The ISACA Blockchain Audit Framework complements this approach with a practical audit program for distributed technologies, emphasizing risk-based trust assessment, regulatory compliance (including GDPR, DORA, and NIS2), and the automation of control mechanisms (Michniewicz, 2021).

In parallel, NIST IR 8202 (2018) – "Blockchain Technology Overview" defines a security framework for blockchain, highlighting the requirements for integrity and tamper resistance, while NIST SP 800-207 (2020) – "Zero Trust Architecture" provides the conceptual foundation for Data Trust models, emphasizing continuous verification, least-privilege principles, and secure data access.

Interoperability and Automation – ISO 22739, IEEE P2418, Compliance-as-Code

The final pillar is interoperability and the automation of rules.

The ISO 22739 standard defines the terminology for interoperable blockchain models, while the IEEE P2418.1–P2418.5 series provides detailed implementation guidelines for specific sectors, including fintech, IoT, supply chain, and healthcare.
Combined with the Compliance-as-Code approach, these standards enable the automatic enforcement of data quality and compliance rules through smart contracts.

As a result, the Data Trust Architecture 3.0 can integrate traditional governance (oversight) with automated auditability, creating a trusted environment for collaboration between organisations and artificial intelligence systems.

Together, these standards form a coherent and interoperable Data Trust Architecture 3.0, where:

- ISO/IEC 8000 and 38505 define data quality and governance frameworks,
- ISO 23258 and 22739 specify semantic interoperability,
- ISO 27001, ISACA, and NIST ensure audit and security mechanisms,
- IEEE P2418 and W3C DIDs introduce technical and automation components.

Collectively, they enable a compliant, accountable, and scalable data trust ecosystem.

Data Trust Architecture

The concept of Data Trust Architecture

In the era of increasing decentralization and automation, the Data Trust Architecture (DTA) serves as the foundation for ensuring integrity, accountability, and interoperability within complex data ecosystems.
The goal of the DTA is to establish a layer of technical and organisational trust that enables the verification of data quality, provenance, and usage, regardless of their source.
This concept originates from the approaches outlined in ISO/IEC 38505 (*Governance of Data*), ISO 22739 (*Blockchain and DLT Vocabulary*), and ISO 27001, which collectively provide a framework for building transparent and auditable data systems.

Layers and roles of the Data Trust Architecture (DTA)

The Data Trust Architecture (DTA) is built upon four interdependent layers that integrate technological, organisational, and regulatory aspects:

Table 2 – Layers of theData Trust Architecture (DTA) and related standards.

Layer	Functional Description	Standards / Reference Frameworks
1. Governance and Policy Layer	Defines data governance principles, responsibilities, quality policies, and lifecycle oversight.	ISO/IEC 38505-1:2017, ISO/IEC TR 38505-2:2018, ISO 8000-61:2016, COBIT 2019 (ISACA), ISACA Blockchain Framework (2021)
2. Identity and Access Layer	Manages data identity, provenance, and access control; includes decentralized identification (DID) and cryptographic key management.	ISO/TS 23258:2021, W3C Decentralized Identifiers (DIDs Core, 2022), NIST SP 800-63C:2020, Regulation (EU) 2024/1183 – eIDAS 2.0
3. Integrity and Provenance Layer	Ensures authenticity and integrity of data through cryptographic proofs and immutable ledgers (DLT).	ISO 22739:2024, ISO/CD TS 23353-2 – Auditing Guidelines for Blockchain and DLT (in development), NIST IR 8202:2018, ISO/IEC 27001:2022
4. Interoperability and Automation Layer	Integrates processes, automates compliance (*Compliance-as-Code*), and enables data exchange across domains (Data Mesh).	ISO/TC 307 JWG 4 – Interoperability of DLT, IEEE P2418.x Series (2018–2024),

Each layer is supported by audit and monitoring mechanisms that enable the continuous assessment of data quality and trust (data trust score).

Key roles within the DTA include:

- Data Owner – responsible for the value and compliance of data;
- Data Steward – ensures data quality and integrity;
- Trust Operator – maintains trust infrastructure (DLT, audit systems);
- Auditor / Regulator – verifies compliance and operational accountability.

Table 3 – Key roles in the Data Trust Architecture

Role	Function Description
Data owner	A legal entity or individual who owns the data and defines policies for its use.
Data steward	Responsible for the quality, compliance, and integrity of data within a specific domain.
Trust authority	An organisation or infrastructure that provides independent verification of data provenance and authenticity (e.g., a blockchain oracle).
Data consumer	A user or system that utilizes data in decision-making processes or AI models.
Auditor / Regulator	Oversees compliance with regulations (e.g., GDPR, DORA, ISO 27001) using distributed ledgers to verify events.

Interoperability and automation of trust

Interoperability represents a key dimension of the Data Trust Architecture (DTA), enabling data exchange across domains, ledgers, and organisations without losing the context of trust.
The application of standards such as ISO 23257:2022 (DLT Reference Architecture) and IEEE P2418.x (Blockchain Frameworks for Industry) allows the creation of meta-communication and semantic layers (*interoperability fabrics*).
The automation of trust rules, for example through smart contracts, enables the dynamic enforcement of data quality and compliance policies (*Compliance-as-Code*), forming a fundamental pillar of Data Governance 3.0.

Blockchain as a technology ensuring integrity, auditability and compliance

In the context of Data Governance 3.0, blockchain constitutes a key component of the Data Trust Architecture (DTA), enabling the creation of systems in which data are immutable, accountable, and compliant with applicable regulations.

According to ISO 22739:2024 – *Blockchain and Distributed Ledger Technologies – Vocabulary*, blockchain is a distributed, tamper-resistant ledger in which data are recorded in a sequence of cryptographically linked blocks, forming a durable and auditable trail.

Integrity

The core mechanism of blockchain is cryptographic hashing combined with the chained structure of blocks, ensuring that any change in a recorded dataset is immediately detectable.

From a data-management perspective, this provides tamper-evidence and the ability to prove that information has not been altered since its creation.

Standards such as ISACA Blockchain Audit Program (ISACA, 2021) and NIST IR 8202 (2018) indicate that distributed ledgers can serve as trust anchors—sources of integrity evidence for external systems (e.g., databases, analytical or reporting systems).
Thus, blockchain does not replace traditional data repositories but reinforces their credibility, creating a cryptographic layer of assurance.

Auditability

Each blockchain entry contains the author's identifier, a timestamp, and a reference to the previous block.
This structure enables complete data lineage tracking and creates an immutable audit trail, consistent with standards such as ISO 20435:2023 – *Auditing Guidelines for Blockchain Systems* and the ISACA Blockchain Framework (2021).
In practice, this means that evidence for internal and external audits can be generated automatically, without relying on a centralized control system.
Every network participant can independently verify the validity of data, in line with the principle of distributed trust.

Compliance

Blockchain supports Compliance-as-Code, allowing access, retention, and data-protection policies to be encoded as smart contracts.
This enables organisations to implement technically verifiable and auditable mechanisms in line with GDPR, ISO/IEC 38505 (Governance of Data), and the DORA regulation.
In federated environments, blockchain can function as a cross-domain accountability layer, allowing different entities (e.g., organisational units, business partners, regulators) to jointly manage trust and data responsibility—consistent with ISO/TC 307 guidelines on interoperability and decentralized identity.

Added Value in the Data Governance 3.0 Architecture

Architecturally, blockchain acts as an independent "data notary", providing:
• integrity – proof that data have not been altered;
• accountability – the ability to assign responsibility for actions;
• compliance – automated enforcement of rules and regulations;
• transparency – a shared, verifiable event view for all stakeholders.

In this way, blockchain not only increases trust in data but also becomes a mechanism for managing the informational value in a decentralized ecosystem—where trust is established through mathematical verifiability rather than institutional authority.

Integration with AI, data mesh and compliance-as-code.

In the era of complex and distributed data ecosystems, the integration of artificial intelligence (AI), Data Mesh architecture, and Compliance-as-Code represents a key direction in the evolution of data management under the Data Governance 3.0 paradigm.
Their convergence enables the transformation of the traditional data governance model into a dynamic, self-regulating system founded on technological trust.

AI as a catalyst for data quality and value

Artificial intelligence is becoming an integral part of Data Governance processes, serving both as an analytical tool and a verification mechanism.
AI models support:
• automatic classification and labeling of data,
• detection of anomalies and inconsistencies in data quality,
• predictive management of information risk.

According to ISO/IEC 42001:2023 - AI Management System Standard and ISO/IEC 38505- Governance of Data, the responsible deployment of AI requires ensuring transparency, auditability, and algorithmic accountability.
In this context, blockchain can serve as a trusted validation layer, storing evidence of data provenance and processing used for training AI models — the so-called data lineage proof.

Data mesh – a federated architecture for data management

The Data Mesh architecture redefines how large organisations manage data by shifting responsibility from central IT teams to business domains.
Each domain becomes a data product provider (Data as a Product), which requires mechanisms for accountability, interoperability, and trust across domains.

In this model, blockchain serves as a federated trust ledger that:
• enables cross-domain accountability, where each team records data changes in an immutable ledger;
• supports semantic interoperability through shared standards such as ISO 23257 and ISO/TS 23258;
• provides cryptographic proof of process compliance with organisational policies.

The integration of Data Mesh and blockchain creates an environment in which data can be shared and governed without compromising their consistency or credibility — forming the foundation of decentralized data governance.

Compliance-as-Code – automation of rules and oversight

In the traditional model, compliance was a reactive process, based on *ex post* audits. Compliance-as-Code (CaC) introduces a proactive approach, in which policies, rules, and standards are expressed as declarative code and automatically enforced in real time.

Blockchain provides an independent enforcement mechanism for CaC through:
• smart contracts implementing compliance rules (e.g., data retention, user access, transaction limits);
• cryptographic compliance logs, auditable in accordance with ISO 20435 and the ISACA Blockchain Framework;
• integration with regulatory frameworks (e.g., GDPR, DORA, AI Act), enabling technical proof of compliance at the data level.

The combination of CaC, AI, and Data Mesh leads to the emergence of self-regulating systems capable of automatically detecting and enforcing non-compliance — forming the foundation of future Data Autonomy Governance.

Towards autonomous and accountable data ecosystems

The integration of AI, Data Mesh, and Compliance-as-Code within the Data Trust Architecture creates a unified environment where:
• AI analyzes and predicts data quality and risk,
• Data Mesh distributes data ownership and accountability,
• Blockchain and CaC ensure automatic accountability and compliance.

As a result, an autonomous, resilient, and auditable ecosystem emerges — one in which trust in data arises from the synergy of people, processes, and technology, rather than from organisational control alone.

Conclusions

The presented concept of Data Governance 3.0 and the developed model of the Data Trust Architecture (DTA) demonstrate that the future of data management will no longer rely solely on centralized oversight, but rather on distributed mechanisms of trust, accountability, and interoperability.
The evolution from Data Governance 1.0 (centralization and control), through 2.0 (federation and automation), to 3.0 (trust and decentralization) defines a new direction for organisations—one in which data become not only an asset, but also a unit of trust and value.

Blockchain and other distributed ledger technologies (DLT), combined with frameworks from ISO, ISACA, and NIST, create an infrastructure of trust that enables:
• ensuring data integrity (proof of immutability and provenance);
• building organisational and technical accountability (complete audit trail);
• strengthening regulatory compliance (*Compliance-as-Code*);
• and integrating with AI and Data Mesh architectures, leading to autonomous data ecosystems.

As such, Data Trust Architecture 3.0 can be regarded as a reference framework for trusted and interoperable data systems, aligned with the directions set by ISO/TC 307 and ISO/IEC 38505.

Despite significant progress, several challenges and research areas require further scientific and technological exploration:

1. Formalization of Data Trust Models
   – development of a unified *data trust score* model integrating quality (ISO/IEC 8000), compliance (ISO/IEC 38505), security (NIST IR 8202), and auditability (ISO 20435) criteria.

2. Semantic and technical interoperability across blockchains
   – further standardization of ISO/TS 23258 and IEEE P2418.x to enable metadata and policy exchange in heterogeneous blockchain networks.

3. AI-driven trust validation
   – leveraging AI models to analyse network behaviour, data usage patterns, and integrity breaches, supporting real-time dynamic trust management.

Within the next decade, Data Governance 3.0 may evolve into Data Trust 4.0 — an integrated, intelligent, and self-enforcing ecosystem where:
• data possess their own identity, value, and history;
• trust is measurable and dynamically verifiable;
• compliance is automated and auditable in real time;
• and the cooperation between humans, systems, and institutions is grounded in open standards and shared definitions of reliability.

References

- AI Act (2024) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Ciupa, K. (2020) Blockchain in three dimensions of value. Warsaw: Difin.
- CRA (2024) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 167/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).
- DAMA International (2017) DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK). 2nd edn. New Jersey: Technics Publications.
- Dehghani, Z. (2022) Data Mesh: Delivering Data-Driven Value at Scale. Sebastopol, CA: O'Reilly Media.
- DORA (2022) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act).
- eIDAS 2.0 (2024) Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
- IEEE (2020) IEEE Standard for the Framework of Blockchain Use (IEEE Std 2418.1-2020). New York: Institute of Electrical and Electronics Engineers.
- ISACA (2005) COBIT 4: Control Objectives for Information and Related Technology. Rolling Meadows, IL: ISACA.
- ISACA (2015) COBIT for Information Security. Rolling Meadows, IL: ISACA.
- ISACA (2021) Blockchain Framework Audit Program. Rolling Meadows, IL: ISACA.

  ISO (2021) ISO/TS 23258:2021 Blockchain and distributed ledger technologies — Taxonomy and ontology for smart contracts. Geneva: International Organization for Standardization.
- ISO (2022) ISO 23257:2022 Blockchain and distributed ledger technologies — Reference architecture. Geneva: International Organization for Standardization.
- ISO (2022) ISO/TS 23635:2022 Blockchain and distributed ledger technologies — Guidelines for governance. Geneva: International Organization for Standardization.
- ISO (2022) ISO 8000-2:2022 Data quality — Part 2: Vocabulary. Geneva: International Organization for Standardization.
- ISO (2024) ISO 22739:2024 Blockchain and distributed ledger technologies — Vocabulary. Geneva: International Organization for Standardization.
- ISO/IEC (2008) ISO/IEC 25012:2008 Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model. Geneva: International Organization for Standardization.
- ISO/IEC (2017) ISO/IEC 38505-1:2017 Information technology — Governance of IT — Governance of data. Geneva: International Organization for Standardization.
- ISO/IEC (2022) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: International Organization for Standardization.
- ISO/IEC (2023) ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system. Geneva: International Organization for Standardization.
- MiCA (2023) Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Markets in Crypto-Assets Regulation).
- Michniewicz, M. (2021) 'Security Auditing of Systems Based on Blockchain Technology', in Technological Aspects of Personal Data Protection. FNCE 2021 Post-Conference Monograph.
- NIS2 (2022) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).

- NIST (2020) NIST Special Publication 800-207: Zero Trust Architecture. Gaithersburg, MD: National Institute of Standards and Technology.
- W3C (2022) Decentralized Identifiers (DIDs) v1.0: W3C Recommendation. World Wide Web Consortium.
- Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018) Blockchain Technology Overview. NIST Interagency/Internal Report (NISTIR 8202). Gaithersburg, MD: National Institute of Standards and Technology.