The FAIR-Blockchain Nexus: A Framework for AI-driven Digital Transformation in the Public Sector

Gideon Mekonnen Jonathan*, Erik Perjons

Department of Computer and Systems Sciences (DSV), Stockholm University, Borgarfjordsgatan 12, SE-16455 Kista, Sweden

Abstract

Public organisations are undergoing rapid digital transformation aimed at enhancing service efficiency, transparency, and accountability. However, persistent challenges remain in managing and reusing data across agencies, as well as in ensuring trust and explainability within Artificial Intelligence (AI)–driven systems. This study examines how the principles of FAIR data management (Findable, Accessible, Interoperable, Reusable) and blockchain technologies can be operationalised within public sector enterprise models to enable transparent, sovereign, and trustworthy AI adoption. Guided by the Technology–Organisation–Environment (TOE) framework and Dynamic Capabilities theory, we conducted a qualitative analysis of interview data from multiple government organisations engaged in AI readiness and digital transformation initiatives. The findings indicate that FAIR and blockchain-related practices are emerging as key enablers of interoperability, provenance, auditability, and data sovereignty. Based on the result of a thematic analysis and theoretical synthesis, the study proposes an enterprise modelling framework that integrates FAIR principles and blockchain mechanisms across the TOE dimensions to support transparent and sovereign AI-driven transformation. The study contributes an actionable model for policymakers and practitioners seeking to align governance, data infrastructure, and technological innovation within public digital ecosystems.

Keywords

Digital Transformation, Public Sector, Enterprise Modeling, FAIR Data, Blockchain, Artificial Intelligence, Data Governance, Digital Sovereignty

1. Introduction

1.1. Background

The continuous adoption of emerging technologies has transformed public administration, enhancing service efficiency, accessibility, and responsiveness [1, 2]. Recently, governments worldwide have accelerated the deployment of artificial intelligence (AI) to support decision-making, streamline administrative processes, and deliver citizen-centred services [3]. Yet, evidence indicates that the benefits of AI adoption in the public sector remain constrained by institutional complexity, regulatory oversight, and ethical accountability [1, 3]. Unlike private enterprises, public organisations operate within tightly regulated environments where issues of data governance, transparency, and interoperability are critical for legitimacy and trust. Consequently, effective AI deployment requires rigorous attention to data quality, explainability, and ethical compliance, as algorithmic systems increasingly influence rights, welfare, and public value [4].

The success of AI-driven digital transformation in government thus hinges on the ability to manage, share, and reuse data across institutional and jurisdictional boundaries. However, despite considerable progress in digitising administrative services, many agencies still function in fragmented data ecosystems, limiting integration and reuse across departments [5, 6]. Such fragmentation undermines coordination and impedes the development of interoperable and transparent AI applications. In this context, the FAIR (Findable, Accessible, Interoperable, and Reusable) data principles provide a framework for improving data stewardship and interoperability [7, 8]. When embedded within enterprise

PoEM2025: Companion Proceedings of the 18th IFIP Working Conference on the Practice of Enterprise Modeling: PoEM Forum, Doctoral Consortium, Business Case and Tool Forum, Workshops, December 3-5, 2025, Geneva, Switzerland.

*Corresponding author.
gideon@dsv.su.se (G. M. Jonathan); perjons@dsv.su.se (E. Perjons)
0000-0001-6360-7641 (G. M. Jonathan); 0000-0001-9044-5836 (E. Perjons)

models, these principles can formalise data management practices, standardise information flows, and promote cross-agency collaboration, thereby supporting evidence-based and reproducible AI-driven public services [9]. At the same time, blockchain technologies are gaining prominence for their potential to enhance trust, transparency, and auditability in multi-stakeholder data environments [10, 11]. By offering immutable ledgers and distributed verification, blockchain enables the tracing of data provenance, ensures integrity, and facilitates verifiable compliance with regulatory frameworks [12]. These capabilities are particularly relevant in federated and cross-jurisdictional public data ecosystems, where coordination across agencies must occur without reliance on a single intermediary [13]. Blockchain can thus act as a technological assurance layer complementing FAIR principles, enabling tamper-evident audit trails and traceable data flows that strengthen accountability and transparency in AI systems [14].

Together, FAIR data management principles and blockchain integration offer a pathway towards trustworthy and sovereign AI-driven digital transformation in the public sector. Embedding these paradigms within enterprise models supports a holistic form of digital transformation in which interoperability, auditability, and transparency are designed into the very architecture of public information systems.

1.2. Research Problem

While the individual merits of the FAIR data principles and blockchain technologies have each garnered considerable scholarly attention, their combined potential within the unique context of public sector digital transformation remains relatively underexplored. Prior studies extensively investigated the benefits of FAIR for improving data stewardship and reusability, for instance, in scientific and research domains [7, 8]. Studies have also explored blockchain's capacity to deliver trust, transparency, and auditability across multi-stakeholder systems [15, 16]. However, a critical empirical gap exists at the intersection of these two research areas. We argue that there is limited work that systematically examines how FAIR principles and blockchain mechanisms intersect to enable the specific demands of AI-driven transformation within public organisations, which require both highly interoperable data and verifiable provenance and accountability [17]. Thus, there is a lack of understanding of how these complementary practices can be systematically integrated and operationalised within formal enterprise modelling frameworks that accurately represent the complex, legacy-laden, and compliance-heavy environments of the public sector. Current models often address technological implementation or governance in isolation, failing to provide a unified, actionable framework that aligns data infrastructure (FAIR), trust mechanisms (blockchain), and organisational strategy to support the adoption of transparent and trustworthy AI. Addressing this knowledge gap is crucial for policymakers and practitioners aiming to transition from pilot projects to a sustainable, accountable, and sovereign public digital ecosystem.

1.3. Aim and Research Questions

This study aims to empirically examine how public organisations can operationalise the FAIR data principles and blockchain-enabled trust mechanisms within AI-driven digital transformation initiatives. The research is guided by the following questions:
1. *How do FAIR data principles and blockchain-related practices manifest within the technological, organisational, and environmental contexts of public sector AI adoption?*
2. *How can these insights be represented within an enterprise modelling framework that supports transparent and sovereign digital transformation?*
3. *What dynamic capabilities enable public organisations to sense, seize, and reconfigure resources for FAIR- and blockchain-aligned AI adoption?*

To address these questions, the study integrates the Technology–Organisation–Environment (TOE) framework [18, 19] and the Dynamic Capabilities theory [20, 21]. The TOE framework provides a basis for understanding the technological infrastructures, organisational readiness, and environmental pressures shaping AI adoption. In turn, Dynamic Capabilities theory elucidates how organisations sense opportunities, seize them through governance and investment, and reconfigure systems and processes to sustain innovation. By combining these perspectives, the study conceptualises FAIR and blockchain integration as *dynamic enablers* within enterprise modelling. Thus, the contribution of this paper is threefold. First, it empirically identifies how FAIR and blockchain-related practices are emerging within public sector AI initiatives. Second, it proposes a novel *Enterprise Modelling Framework for FAIR–Blockchain–AI Integration*, grounded in the TOE and Dynamic Capabilities perspectives. Third, it offers actionable implications for policymakers and enterprise architects seeking to design transparent, interoperable, and sovereign digital systems.

The remainder of this paper is organised as follows. The next section reviews the extant literature, outlining the theoretical bases of the study—the TOE framework and the Dynamic Capabilities perspective—and examining how FAIR data management, blockchain, and AI adoption intersect in the public sector to enhance transparency, interoperability, and digital sovereignty. The subsequent section describes the research methodology, including data collection and analysis methods. The results section presents key findings from thematic analysis of the qualitative data. The discussion interprets these findings through the combined TOE–Dynamic Capabilities lens, leading to a FAIR–Blockchain enterprise modelling framework. The paper concludes by summarising main contributions, implications for research and practice, limitations, and future research directions.

2. Related Work

2.1. Theoretical Foundation

Prior studies, within the context of private firms, have widely employed the Technology–Organisation–Environment (TOE) framework to examine the determinants of technology adoption across organisations [18, 19, 22]. Within the public sector, researchers argue that it offers a structured lens for analysing how technological infrastructures, organisational readiness, and environmental factors, including regulation, policy, and inter-agency coordination, jointly shape digital transformation [23, 24]. The TOE framework thus provides a valuable basis for understanding how emerging technologies such as AI, FAIR data infrastructures, and blockchain systems are introduced and assimilated within government settings. However, TOE primarily explains adoption drivers and contextual enablers; it does not sufficiently account for the dynamic, path-dependent processes through which organisations evolve and continuously adapt to technological change [25].

To address this limitation, the Dynamic Capabilities (DC) perspective offers a complementary lens by emphasising the adaptive and evolutionary nature of organisational transformation [20, 21]. According to Teece et al. [20], dynamic capabilities refer to an organisation's ability to *sense* new opportunities and threats, *seize* them through strategic decisions and resource mobilisation, and *reconfigure* existing structures and competencies to sustain long-term performance in changing environments. This theory has been increasingly applied to digital transformation research, where organisations must balance technological innovation with institutional constraints [26, 27]. In the public sector, dynamic capabilities have been linked to the ability to institutionalise new governance practices, develop data-driven decision-making routines, and respond flexibly to regulatory and ethical demands [1, 3].

Integrating TOE and DC perspectives enables a more comprehensive understanding of public sector digital transformation by linking the *structural determinants* of adoption (as captured by TOE) with the *processual mechanisms* of adaptation and renewal (as described by DC). In the context of this study, the combined framework is used to conceptualise how public organisations operationalise the FAIR data principles and blockchain-based trust mechanisms within AI-driven enterprise modelling. TOE provides insight into the technological, organisational, and environmental conditions shaping the adoption of these mechanisms, while DC illuminates how institutions cultivate sensing, seizing, and reconfiguring capabilities to embed them sustainably. Together, these perspectives support a dynamic and multi-level analysis of how interoperability, transparency, and digital sovereignty can be institutionalised through FAIR–Blockchain integration in public sector enterprise systems.

2.2. FAIR Data Principles and Data Governance

The FAIR data principles—Findable, Accessible, Interoperable, and Reusable—were initially formulated to guide the management and stewardship of scientific research data [8, 7]. They have since gained prominence across sectors as a foundational framework for ensuring that data assets are both machine-actionable and human-interpretable [8]. In the context of public administration, FAIR principles provide a conceptual and operational blueprint for improving data quality, discoverability, and interoperability across organisational boundaries [6]. Their implementation requires the establishment of standardised metadata schemas, persistent identifiers, open application programming interfaces (APIs), and institutionalised data stewardship functions that together facilitate systematic data governance [9].

Within the context of public sector and government data systems, FAIR adoption has been increasingly recognised as a prerequisite for AI readiness and data-driven innovation and transformation [28, 29]. The results from prior empirical studies demonstrate that FAIR-aligned data infrastructures enable efficient data integration and reuse across administrative domains, thereby enhancing the transparency, accountability, and reusability of public data resources [30]. The rationale is that when embedded into enterprise architectures, FAIR principles help establish common vocabularies, shared ontologies, and open standards that promote interoperability between disparate systems, improving both data quality and the traceability of algorithmic decisions [31].

However, despite their growing relevance, the findings of prior studies indicate that the implementation of FAIR principles in the public sector remains uneven and fraught with institutional and technical challenges [32, 5]. For instance, according to the data from the European Commission, legacy systems, proprietary software dependencies, and inconsistent metadata standards continue to hinder the establishment of coherent data ecosystems [33]. Moreover, public organisations often lack the governance maturity and skilled data stewardship necessary to operationalise FAIR compliance at scale [34]. The fragmentation of responsibilities across ministries and agencies is also recognised as a concern that exacerbates this issue, resulting in siloed data practices and limited reuse of government datasets. We argue that addressing these challenges requires the integration of FAIR principles within broader data governance frameworks that align organisational structures, technological infrastructures, and policy instruments. This alignment transforms FAIR from a set of technical recommendations into an institutional mechanism for achieving transparency, interoperability, and trust in digital government. In this study, FAIR is therefore conceptualised not merely as a data management guideline but as a *governance paradigm*—one that enables public organisations to move towards accountable, sustainable, and AI-ready data ecosystems.

2.3. Blockchain for Transparency, Accountability, and Sovereignty

Blockchain technology provides a distributed, tamper-evident ledger that enables secure, transparent, and auditable record-keeping across organisational boundaries[35]. By design, blockchain systems ensure that transactions are recorded chronologically and cryptographically verified, reducing the need for central intermediaries and enhancing the integrity of shared information [36]. The application of blockchain technology in public administration has been a topic of discussion among researchers and practitioners [37]. Most recently, blockchain applications have become a reality in domains such as identity management, public procurement, land registration, and data provenance, where transparency and accountability are essential [10, 11]. These implementations demonstrate blockchain's capacity to strengthen institutional trust by making transactions verifiable and resistant to ex-post alteration.

From a governance perspective, blockchain offers mechanisms that can reinforce compliance, traceability, and accountability across complex data ecosystems [12]. Immutable ledgers and smart contracts enable automated policy enforcement, providing audit trails that align with regulatory requirements. When combined with FAIR-aligned data infrastructures, blockchain supports the provenance and authenticity of shared datasets, ensuring that data flows can be traced to their origin while maintaining verifiable consent and usage conditions [38]. This synergy is particularly relevant for AI-driven systems, where explainability and accountability depend on the ability to reconstruct data lineage and model provenance [14]. Beyond its technical affordances, blockchain also has profound implications for digital sovereignty—the ability of public institutions and nations to exercise control over their digital infrastructures, data assets, and algorithmic systems [4]. By decentralising data storage and governance, blockchain reduces reliance on proprietary platforms and external cloud providers, thus mitigating risks of vendor lock-in and foreign dependency [13]. In cross-border digital collaborations, distributed ledger systems can serve as trusted coordination mechanisms that preserve local autonomy while enabling secure interoperability between jurisdictions [37, 39]. Consequently, blockchain aligns with the broader goals of sovereign digital transformation by embedding trust and accountability directly into the local technological infrastructure [40].

However, it is worth noting that significant challenges need to be tackled before blockchain can be widely institutionalised within public-sector ecosystems [37]. Technical limitations such as scalability, interoperability, and energy efficiency continue to constrain adoption [41]. Moreover, issues of legal interoperability, data protection compliance (e.g., GDPR), and governance accountability pose non-trivial policy challenges [42, 43]. To address these concerns, public organisations must adopt a socio-technical approach that integrates blockchain deployment with regulatory adaptation, ethical oversight, and institutional learning. Within this study, blockchain is therefore conceptualised not solely as a technological artefact but as a *governance infrastructure*—one that operationalises transparency, accountability, and digital sovereignty within FAIR-aligned, AI-enabled enterprise systems.

2.4. Integrating FAIR and Blockchain

Recent research highlights the growing convergence between the FAIR data principles and blockchain technologies as complementary approaches to achieving trustworthy, interoperable, and transparent data ecosystems [44, 45]. The FAIR principles provide a framework for ensuring that data is findable, accessible, interoperable, and reusable, while blockchain offers distributed and immutable infrastructures that enhance data integrity, provenance, and verifiability [46]. When integrated, these two paradigms can mutually reinforce each other, bridging the gap between data management best practices and decentralised trust mechanisms.

From a technical perspective, blockchain can strengthen FAIR implementation by embedding *provenance metadata* directly within distributed ledgers, thereby securing the authenticity and lineage of datasets [47]. For instance, smart contracts enable automated access control and consent management, ensuring that FAIR principles such as accessibility and reusability are operationalised in a verifiable and auditable manner. Immutable ledger entries, on the other hand, support reproducibility and accountability in AI pipelines by maintaining transparent records of model training data, algorithmic parameters, and validation processes. Prior studies suggest that such capabilities are increasingly recognised as essential for ethical AI governance and compliance with emerging regulatory frameworks such as the EU AI Act [4]. Moreover, FAIR-compliant metadata and data stewardship practices enhance the *usability and interoperability* of blockchain-stored assets [48]. Standardised metadata schemas, persistent identifiers, and open ontologies make blockchain-registered datasets discoverable and machine-readable across platforms. This integration transforms blockchain from a transaction-centric technology into a data-centric infrastructure capable of supporting scientific reproducibility, cross-domain collaboration, and long-term data preservation [49]. In the context of public sector AI, this synergy allows for transparent, traceable, and reusable data flows, thereby enabling responsible algorithmic decision-making and reducing information asymmetries between institutions and citizens. Beyond technical alignment, integrating FAIR and blockchain embodies a *socio-technical paradigm* of data governance that embeds accountability and transparency within the architecture of public digital systems [50].

In summary, FAIR principles provide the semantic and procedural foundations for effective data management, while blockchain offers the infrastructural assurances of integrity, provenance, and sovereignty. When combined within enterprise modelling, these mechanisms enable governments to design AI systems that are not only efficient and interoperable but also ethically robust and publicly verifiable. Thus, the FAIR–Blockchain integration offers a pathway towards achieving sustainable, sovereign, and trustworthy AI ecosystems in the public sector.

2.5. Enterprise Modelling as an Enabler of AI-driven Digital Transformation

Digital transformation in the public sector extends far beyond the adoption of new technologies; it entails the comprehensive reconfiguration of organisational structures, service delivery processes, and policy frameworks [1]. It involves aligning institutional capacities, regulatory instruments, and technological infrastructures to enhance transparency, efficiency, and public value creation [2]. Within this context, *enterprise modelling* has emerged as a crucial analytical and design approach for capturing the interdependencies between organisational processes, information systems, and governance mechanisms that drive digital change [51, 52]. Through formal representations of processes and data flows, enterprise models enable public organisations to align strategic objectives with operational capabilities and to simulate the impact of technological interventions before implementation. However, existing enterprise models often fail to incorporate evolving paradigms of data governance and distributed trust. Traditional models were primarily developed for static and centralised architectures, offering limited support for modelling federated and adaptive data ecosystems characteristic of modern public administration [53]. As emerging frameworks such as FAIR data management and blockchain-enabled trust mechanisms gain prominence, there is a growing need for enterprise modelling approaches that reflect interoperability, provenance, and accountability as integral design dimensions [54]. Embedding these principles into enterprise models allows governments to represent not only organisational and technical systems but also the normative and ethical infrastructures that underpin trustworthy digital transformation.

In this study, enterprise modelling is employed as a conceptual and analytical framework to integrate the *Technology–Organisation–Environment (TOE)* and *Dynamic Capabilities (DC)* perspectives, enabling the systematic representation of how FAIR and blockchain mechanisms can be institutionalised within AI-driven public sector transformation. Embedding these principles into enterprise models allows governments to represent not only organisational and technical systems but also the normative and ethical infrastructures that underpin trustworthy digital transformation.

3. Research Methodology

This study adopts a qualitative, interpretivist research design to examine how the FAIR data principles and blockchain-related mechanisms are shaping AI adoption within public organisations. A qualitative approach is particularly appropriate for investigating emerging socio-technical phenomena where context, perception, and institutional dynamics are central to understanding complex processes [55]. Interpretivism assumes that social reality is constructed through the meanings and interactions of participants, making it suitable for studies seeking to capture the lived experiences and sense-making of public officials involved in digital transformation [56].

The data collection is conducted through semi-structured interviews with senior officials, data managers, and digital transformation officers from multiple ministries and government agencies across Kenya. Participants were selected based on their involvement in national AI readiness, data governance, and policy coordination initiatives. Participants represented a range of public organisations, including ministries responsible for Information and Communication Technology (ICT), finance, planning, and regulatory oversight. Each interview lasted between 45 and 60 minutes and was conducted via Zoom. The interview guide covered topics including data management practices, AI strategy implementation, governance frameworks, and interoperability challenges. The cross-institutional focus enabled comparative insights into how technological, organisational, and environmental factors influence FAIR and blockchain integration within AI-related programmes. This design aligns with established qualitative methodologies in digital government and information systems research, which emphasise depth of insight over statistical generalisation [57].

The data analysis followed a thematic coding approach guided by the TOE framework and the Dynamic DC theory. This dual-theoretical lens provided a structured means of examining both the contextual determinants of adoption and the adaptive processes of organisational learning [21, 19]. The analysis focused specifically on segments related to FAIR data management and blockchain-aligned mechanisms such as data provenance, auditability, transparency, and digital sovereignty. A hybrid deductive–inductive coding strategy was employed. Deductive codes were derived from established TOE–DC constructs, while inductive codes emerged from the empirical data to capture novel insights. The final coding matrix (see Table 1 in the supplementary material) consisted of 14 major themes distributed across the technological, organisational, and environmental contexts. Each theme was subsequently mapped to corresponding dynamic capabilities—sensing, seizing, and reconfiguring—to elucidate how public organisations identify, mobilise, and adapt resources in response to governance challenges. Short, representative quotations were retained to preserve authenticity and contextual richness.

4. Results

The analysis of interview data generated insights into how public organisations are engaging with FAIR data management and blockchain-related mechanisms as integral components of their wider AI adoption and digital transformation initiatives. Using the TOE framework as an interpretive lens, three core dimensions emerged, each reflecting the contextual forces shaping digital governance. Within each dimension, respondents described practices and constraints corresponding to the Dynamic Capabilities of sensing, seizing, and reconfiguring. View the thematic coding framework here.

4.1. Technological Context (Fragmentation, FAIR Maturity, and Infrastructure Renewal)

Across all participating agencies, respondents acknowledged steady progress in data digitisation and improvements in data quality, but they also highlighted persistent fragmentation between systems and departments. One participant observed that "*data availability is improving … but integration remains challenging due to different systems and standards across agencies.*" This fragmentation limits the realisation of the FAIR principles—particularly interoperability and reusability—which are essential for developing comprehensive AI datasets and models. Another official commented that "*data quality for our AI applications is generally good, but challenges remain in accessing comprehensive data across all government agencies.*" While individual institutions have modernised their local data infrastructures, cross-agency integration remains weak, hindering the development of national-scale AI capabilities and collaborative analytics.

In response, several ministries have begun implementing the National Data Management Framework (NDMF), which introduces governance standards, metadata stewardship roles, and inter-agency coordination mechanisms. These efforts represent organisational seizing capabilities—concrete attempts to operationalise FAIR accessibility and interoperability through structured governance and dedicated stewardship functions. Metadata stewards were identified as pivotal actors in enforcing consistency and quality, translating abstract FAIR principles into daily data practices and institutional norms. However, legacy infrastructures remain a major obstacle. Respondents described incompatibilities between outdated databases and new interoperability standards, as well as limited automation in data cataloguing. These difficulties indicate the need for systematic reconfiguration involving both technical modernisation (e.g., adoption of APIs, deployment of metadata registries) and organisational adaptation (e.g., redefining custodianship roles and harmonising workflows).

Overall, the findings reveal incremental but uneven FAIR maturity across public organisations—notable advances in governance structures and stewardship capacity, yet incomplete interoperability between data ecosystems. The technological layer is evolving towards more structured, FAIR-aligned infrastructures, but the achievement of seamless, cross-ministerial data reusability remains a continuing challenge requiring sustained investment and institutional coordination.

4.1.1. Organisational Context (Privacy, Accountability, and Sovereignty)

Within the organisational context, respondents emphasised that privacy and accountability are no longer peripheral concerns but central design imperatives in the development of AI systems. One senior official explained that "*stringent security and privacy requirements limit AI design options, alongside the need for explainable AI systems that can justify compliance decisions.*" These privacy-by-design and explainability expectations have transitioned from aspirational policy goals into enforceable architectural principles. Thus, the responses indicate that agencies are embedding transparency and traceability into data pipelines, ensuring that every stage of data collection, processing, and model inference is logged and reviewable. These practices align with FAIR's emphasis on documentation, provenance, and traceability. Respondents also highlighted the potential of blockchain to complement such mechanisms through immutable ledgers and tamper-evident provenance tracking, offering verifiable assurance of compliance and accountability.

A second theme within this dimension is related to organisational sovereignty. A regulatory manager noted, "*External vendors assist us, but we maintain strict data sovereignty and security requirements.*" This statement reflects a deliberate strategy to preserve control over data assets and to avoid vendor lock-in—a stance that resonates with blockchain's principles of decentralised trust and distributed control. Sovereignty thus functions simultaneously as a protective mechanism and a strategic enabler, allowing ministries to collaborate across boundaries while retaining autonomy over their data and infrastructure.

Respondents also stressed the enduring importance of human oversight in regulatory AI contexts. As one participant remarked, "*We must maintain strong human accountability mechanisms.*" This awareness underscores a cautious approach to automation in public decision-making, ensuring that algorithmic recommendations remain subject to human judgment, particularly when rights and welfare are at stake. Collectively, these perspectives point to ongoing organisational reconfiguration, where accountability, sovereignty, and transparency are being embedded into internal structures and processes rather than imposed through external compliance mandates. The organisational layer, therefore, reflects both the seizing of new governance capabilities and the reconfiguration of legacy accountability systems to align with emerging digital ethics standards.

4.1.2. Environmental Context (Regulation, Harmonisation, and Cross-Border Collaboration)

At the environmental level, respondents perceived regulatory frameworks as both constraints and catalysts for digital transformation. One official observed that "*the Data Protection Act emphasises privacy by design and algorithmic accountability.*" Such legislation imposes external compliance pressures but simultaneously encourages organisations to adopt FAIR-aligned and auditable systems, thereby reinforcing ethical design and traceability norms across government.

Other respondents underscored the importance of harmonised AI governance frameworks and technical standards to promote consistency among ministries and agencies. Fragmented standards were said to inflate compliance costs and impede interoperability, whereas harmonisation was viewed as a mechanism for reducing redundancy and promoting cross-agency data exchange. By establishing shared reference architectures and legal clarity, harmonised frameworks create enabling conditions under which FAIR and blockchain mechanisms can scale nationally.

A further recurring theme was the importance of cross-border collaboration and regional data governance. As one participant explained, "*...improved cross-border data-sharing agreements would enable more comprehensive AI applications across the public sector.*" This sentiment reflects a growing awareness that AI-enabled public services depend increasingly on regional data ecosystems, requiring not only interoperability but also shared accountability mechanisms. In this regard, respondents viewed blockchain's verifiable credentials and distributed ledgers as promising tools for cross-jurisdictional compliance, allowing machine-verifiable trust between governments and partner institutions.

Collectively, the findings related to the environmental context reveal a dynamic interplay between regulation and innovation. In other words, legal frameworks and policy directives do not merely constrain organisational behaviour. They also drive the institutionalisation of FAIR-aligned data stewardship and stimulate experimentation with blockchain-enabled transparency. The environmental layer thus exemplifies the sensing capability—where organisations interpret and respond to evolving legal, ethical, and geopolitical expectations that shape the governance of AI-driven transformation.

In summary, across the technological, organisational, and environmental dimensions, the findings demonstrate how FAIR data management and blockchain mechanisms are becoming embedded within the evolving digital architectures of public administration. These practices exemplify how sensing, seizing, and reconfiguring capabilities fuse to support ethical, interoperable, and sovereign AI ecosystems. While progress remains uneven, the convergence of FAIR and blockchain principles is fostering a new mode of digital governance—one characterised by verifiable transparency, institutional accountability, and adaptive learning across the public sector.

5. Discussion

The analysis of our interview data reveals how FAIR data principles and blockchain-related mechanisms are being institutionalised within public sector digital transformation, and how these practices resonate with or extend prior research. The findings also suggest that public organisations are progressively embedding the FAIR and blockchain paradigms as dual enablers of transparency, interoperability, and sovereignty of an AI-driven digital transformation.

5.1. Advancing FAIR Maturity and Blockchain Integration (Technological Context)

The results reveal that technological progress in public organisations is characterised by incremental but uneven FAIR maturity. Respondents reported improvements in data quality, metadata management, and the implementation of national data frameworks, such as the NDMF; however, they also emphasised enduring fragmentation and legacy infrastructure challenges. These findings are consistent with prior studies, which demonstrate that technical interoperability remains one of the most persistent barriers to digital transformation in the public sector [2, 5]. As with earlier evidence from European open data initiatives [6], the technological constraints identified here underscore the difficulty of harmonising diverse information systems across ministries and agencies.

FAIR-aligned infrastructures, particularly metadata catalogues, persistent identifiers, and open APIs, were recognised as critical components for ensuring data findability and accessibility. Similar observations are reported by researchers [9] and [30], who found that FAIR-compliant metadata directly improves data reusability and discoverability across research and administrative domains. The technological dimension of this study, therefore, exemplifies a gradual evolution from data digitisation towards data stewardship, a shift also previously identified [34]. However, as a study [32] cautions, FAIR implementation must extend beyond technical compliance to include governance mechanisms that ensure accountability and sustainability.

Blockchain emerged as a complementary technological enabler, particularly in terms of data provenance, auditability, and immutability. Respondents' discussions of blockchain-based verification and logging mechanisms align with previous findings [10, 11], which highlight blockchain's potential to enhance data integrity and reduce transactional opacity in public administration. These technological developments reflect what authors [20, 21] describe as the process of *reconfiguring capabilities*—the capacity of organisations to modernise and realign infrastructures in response to changing technological and policy demands. In this study, reconfiguration involves both infrastructural renewal and the institutionalisation of FAIR—compatible data architectures that can support interoperable and accountable AI ecosystems.

5.2. Embedding Privacy, Accountability, and Sovereignty (Organisational Context)

At the organisational level, the findings indicate that privacy, accountability, and digital sovereignty are becoming central organising logics for AI governance. This mirrors global trends in digital government research that emphasise transparency, explainability, and citizen trust as the ethical foundations of algorithmic decision-making [3]. The integration of privacy-by-design principles and explainable AI architectures demonstrates that public agencies are moving from compliance-oriented practices towards proactive accountability mechanisms. These developments are consistent with the findings of a prior study [4], which found that trustworthy AI depends on verifiable processes of explanation, documentation, and oversight.

Blockchain's perceived role as an accountability infrastructure also parallels findings in the extant literature. For example,[12] and [14] show that distributed ledgers can embed transparency and traceability directly within organisational workflows, reducing information asymmetries and reinforcing procedural fairness. The present study extends these insights by situating blockchain within the FAIR governance ecosystem, revealing how immutable logs can support FAIR's emphasis on provenance and data reuse. Together, these mechanisms illustrate what the DC perspective terms *seizing capabilities*—the mobilisation of resources and governance structures to institutionalise transparency and trust across organisational boundaries.

The emphasis on data sovereignty and the avoidance of vendor lock-in reflect a distinctive strategic orientation in the public sector. Respondents' insistence on retaining control over infrastructure and data aligns with prior studies [13, 40], which describe digital sovereignty as a response to dependency on external vendors and foreign technologies. This sovereignty-driven approach not only safeguards autonomy but also aligns with FAIR's principle of reusability, enabling governments to retain the value of their data assets within national ecosystems. In DC terms, this represents both seizing and reconfiguring processes, wherein public agencies strengthen internal governance while adapting operational routines to new data-sharing norms.

The continued emphasis on human oversight underscores the hybrid nature of AI-enabled public administration—one that combines automation with institutional accountability. Similar insights have been reflected in the findings of previous studies [54], where the authors note that sustaining public trust requires embedding human judgment into digital systems. This study contributes to the discourse by demonstrating how human accountability mechanisms co-evolve with technological innovations, thereby reinforcing the ethical underpinnings of algorithmic governance.

5.3. Regulation, Harmonisation, and Collaboration (Environmental Dimension)

The environmental findings demonstrate that regulatory frameworks act as both external constraints and dynamic catalysts for innovation. The role of data protection and algorithmic accountability legislation as stimuli for FAIR adoption corroborates prior research emphasising that regulation can drive responsible digital transformation [2, 3]. The "privacy by design" mandates described by respondents reflect broader European and African efforts to embed ethical principles into data governance structures [4, 28]. These external pressures exemplify *sensing capabilities*, as organisations monitor and interpret changes in the legal and policy environment to guide adaptive responses.

Harmonised standards and cross-ministerial coordination were identified as essential for scaling FAIR and blockchain mechanisms in the public sector. This observation resonates with prior studies [24, 19], which found that inter-organisational alignment is a decisive factor in technology adoption within the public sector. The implementation of shared governance frameworks, such as the NDMF, illustrates the emergence of what authors, for instance [26], term dynamic alignment processes—structures that enable learning and adaptation across institutional boundaries. By formalising interoperability and metadata standards, these frameworks enable the translation of FAIR principles into enforceable policy instruments.

The emphasis on cross-border data-sharing and regional digital cooperation expands the environmental perspective to include geopolitical and transnational considerations. Respondents' calls for verifiable cross-jurisdictional audit mechanisms reflect the literature on blockchain-enabled data sovereignty [39, 13]. Distributed ledger technologies can, in principle, enable decentralised trust across national boundaries, facilitating the exchange of data and services without relinquishing local control. This finding extends previous research by demonstrating how regional data ecosystems may evolve through the co-implementation of FAIR and blockchain principles—an emerging domain that warrants further empirical attention.

5.4. Integrating TOE and Dynamic Capabilities

Taken together, the findings provide empirical evidence that FAIR and blockchain mechanisms are being institutionalised through multi-level interactions across technological, organisational, and environmental contexts. This confirms the analytical value of integrating the TOE and DC perspectives in explaining AI-driven digital transformation within complex, multi-actor public systems. The TOE framework captures the structural determinants—technological infrastructures, organisational capacities, and environmental pressures—while DC theory illuminates the dynamic processes by which organisations sense opportunities, seize resources, and reconfigure systems for long-term sustainability [21, 27].

In technological terms, sensing and reconfiguring capabilities were evident in the recognition of interoperability challenges and the subsequent adoption of FAIR infrastructures. Within organisations, seizing and reconfiguring manifest through the creation of data stewardship roles and accountability structures that operationalise FAIR and blockchain principles. In terms of environment, sensing capabilities were displayed in the interpretation of regulatory signals and regional cooperation incentives that drive innovation. This dynamic interplay aligns with a study [26], which describes digital transformation as a process of continuous organisational renewal enabled by learning, coordination, and strategic adaptation.

By embedding FAIR and blockchain within this dual-theoretical frame, the study advances an understanding of how AI-driven digital transformation in the public sector is both constrained and enabled by institutional context. It demonstrates that technical interoperability, data sovereignty, and ethical governance are not isolated outcomes but interdependent capabilities that evolve collectively through sensing, seizing, and reconfiguring processes. In doing so, it contributes to the literature on enterprise modelling by offering an empirically grounded model of how FAIR and blockchain can be represented as modular governance components within public data architectures [51, 52, 53].

5.5. Proposed Conceptual Enterprise Model

Building upon the insights above, the study synthesises the empirical findings and theoretical perspectives into a conceptual enterprise model. This model integrates the TOE dimensions with dynamic capability processes to explain how FAIR and blockchain mechanisms can be institutionalised within AI-driven public sector transformation. The following section presents this model, illustrating its structural and functional components.

At its core, the model conceptualises AI-driven digital transformation as a cyclical and evolutionary process. The *technological context* encompasses infrastructures, standards, and data architectures that support FAIR-aligned interoperability and blockchain-enabled provenance. The *organisational context* captures governance structures, stewardship roles, and accountability mechanisms that operationalise these principles within public institutions. The *environmental context* encompasses the regulatory, institutional, and socio-political factors that shape pressures and incentives for the adoption of responsible AI.

Dynamic Capabilities—*sensing*, *seizing*, and *reconfiguring*—operate across these layers as the mechanisms through which organisations interpret external stimuli, mobilise resources, and continuously adapt infrastructures and governance routines [21, 26]. FAIR principles guide data stewardship and interoperability, while blockchain provides technological assurances of provenance, auditability, and digital sovereignty [7, 9, 13]. Together, these mechanisms enable governments to move from fragmented and compliance-driven data management towards adaptive, transparent, and sovereign digital ecosystems.

The framework, therefore, contributes a dynamic enterprise modelling approach, depicting how technical, organisational, and environmental forces interact with capability-building processes to embed trust and accountability into the design of public information systems. It also provides a diagnostic

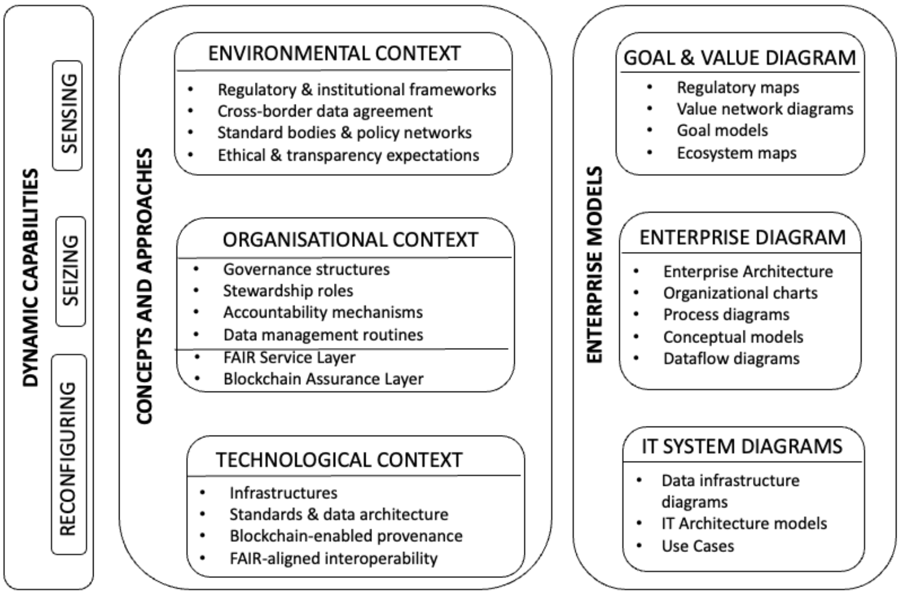

Figure 1: Conceptual Framework

structure for assessing FAIR and blockchain maturity across government agencies, thereby linking conceptual understanding with practical implementation.

6. Concluding Remarks

This study has explored how the FAIR data principles and blockchain-related practices materialise within the technological, organisational, and environmental contexts of public sector AI adoption. By situating these developments within the TOE and DC frameworks, the research demonstrates that the transition toward responsible and sovereign AI is not merely a technical undertaking but a multidimensional process of institutional adaptation and learning.

From a theoretical perspective, the study bridges previously distinct domains—data governance, digital sovereignty, and dynamic capability theory—through a unified conceptual lens. It demonstrates that FAIR principles and blockchain mechanisms operate as complementary governance instruments— FAIR ensures semantic and procedural transparency, while blockchain strengthens integrity, provenance, and sovereignty. Within the TOE–DC framework, these mechanisms illuminate how public organisations transform structural constraints into dynamic opportunities for innovation. The findings extend dynamic capability theory by evidencing how sensing, seizing, and reconfiguring processes underpin not only strategic adaptation but also ethical and institutional renewal. Furthermore, by situating FAIR and blockchain within enterprise modelling, the study contributes to digital governance scholarship by conceptualising how technical and organisational layers interact to enable transparent and accountable data ecosystems.

From a practical standpoint, the research provides actionable insights for policymakers, digital strategists, and public sector leaders seeking to embed responsible AI practices. It proposes that adopting FAIR and blockchain-aligned systems requires not only technological investment but also organisational capability development and regulatory alignment. The enterprise modelling framework introduced here offers a practical tool for visualising interdependencies between data standards, governance roles, and technological infrastructures. Through such modelling, public organisations can anticipate governance bottlenecks, strengthen accountability structures, and enhance inter-agency collaboration. In doing so, the framework enables decision-makers to operationalise principles of transparency, interoperability, and sovereignty in concrete organisational settings.

The study also identifies key dynamic capabilities that enable public organisations to sense, seize, and reconfigure resources in response to evolving digital ecosystems. The capacity to sense emerging technologies and ethical imperatives allows organisations to interpret environmental signals effectively. Seizing involves mobilising investments and partnerships that align with FAIR and blockchain principles, while reconfiguring reflects the ongoing transformation of institutional routines, data infrastructures, and governance norms. Together, these processes highlight that sustainable AI adoption is as much about cultivating adaptive and learning-oriented institutions as it is about deploying advanced technologies.

In conclusion, this research provides a holistic framework for understanding and guiding FAIR- and blockchain-aligned AI adoption in the public sector. It demonstrates that transparent, sovereign, and ethically grounded digital transformation depends on the interplay between technological infrastructures, organisational capabilities, and institutional values. By combining theoretical synthesis with practical modelling tools, the study contributes to both academic inquiry and public governance practice—offering a roadmap for designing trustworthy, resilient, and future-ready public sector AI systems.

Declaration on Generative AI

During the preparation of this work, the authors utilised the GEN AI Tool ChatGPT and Grammarly to check grammar and spelling, paraphrase, and reword. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] I. Mergel, N. Edelmann, N. Haug, Defining digital transformation: Results from expert interviews, Government Information Quarterly 36 (2019) 101385.

[2] G. Vial, Understanding digital transformation: A review and a research agenda, The Journal of Strategic Information Systems 28 (2019) 118–144.

[3] D. Valle-Cruz, J. R. Gil-Garcia, R. Sandoval-Almazan, Artificial intelligence algorithms and applications in the public sector: A systematic literature review based on the prisma approach, Research Handbook on public management and artificial intelligence (2024) 8–26.

[4] L. Floridi, Establishing the rules for building trustworthy ai, in: Ethics, governance, and policies in artificial intelligence, Springer, 2021, pp. 41–45.

[5] M. Young, L. Rodriguez, E. Keller, F. Sun, B. Sa, J. Whittington, B. Howe, Beyond open vs. closed: Balancing individual privacy and public accountability in data sharing, in: Proceedings of the Conference on Fairness, Accountability, and Transparency, 2019, pp. 191–200.

[6] European Commission, Turning fair into reality: Final report and action plan from the european commission expert group on fair data, 2018.

[7] M. D. Wilkinson, M. Dumontier, I. J. Aalbersberg, G. Appleton, M. Axton, A. Baak, N. Blomberg, J.-W. Boiten, L. B. da Silva Santos, P. E. Bourne, et al., The fair guiding principles for scientific data management and stewardship, Scientific data 3 (2016) 1–9.

[8] B. Mons, Data stewardship for open science: Implementing FAIR principles, Chapman and Hall/CRC, 2018.

[9] A. Jacobsen, R. de Miranda Azevedo, N. Juty, D. Batista, S. Coles, R. Cornet, et al., Fair principles: Interpretations and implementation considerations, Data Intelligence 2 (2020) 10–29.

[10] J. Berryhill, T. Bourgery, A. Hanson, Blockchains unchained: Blockchain technology and its use in the public sector, OECD Working Papers on Public Governance (2018).

[11] D. Cagigas, J. Clifton, D. Diaz-Fuentes, M. Fernández-Gutiérrez, Blockchain for public services: A systematic literature review, IEEE access 9 (2021) 13904–13921.

[12] F. Lumineau, W. Wang, O. Schilke, Blockchain governance—a new way of organizing collaborations?, Organization Science 32 (2021) 500–521.

[13] K. Ziolkowska, Distributing authority–state sovereignty in the age of blockchain, International Review of Law, Computers & Technology 35 (2021) 116–130.

[14] R. Asif, S. R. Hassan, G. Parr, Integrating a blockchain-based governance framework for responsible ai, Future Internet 15 (2023) 97.
[15] H. Gamage, H. Weerasinghe, N. Dias, A survey on blockchain technology concepts, applications, and issues, SN Computer Science 1 (2020) 114.
[16] E. J. Hartelius, "the great chain of being sure about things": blockchain, truth, and a trustless network, Review of Communication 23 (2023) 21–37.
[17] T. Birkstedt, M. Minkkinen, A. Tandon, M. Mäntymäki, Ai governance: themes, knowledge gaps and future agendas, Internet Research 33 (2023) 133–167.
[18] L. G. Tornatzky, M. Fleischer, The Processes of Technological Innovation, Lexington Books, Lexington, MA, 1990. ISBN 978-0669203486.
[19] A. Al Hadwer, M. Tavana, D. Gillis, D. Rezania, A systematic review of organizational factors impacting cloud-based technology adoption using technology-organization-environment framework, Internet of Things 15 (2021) 100407.
[20] D. J. Teece, G. Pisano, A. Shuen, Dynamic capabilities and strategic management, Strategic Management Journal 18 (1997) 509–533.
[21] D. J. Teece, Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance, Strategic Management Journal 28 (2007) 1319–1350.
[22] H. Felemban, M. Sohail, K. Ruikar, Exploring the readiness of organisations to adopt artificial intelligence, Buildings 14 (2024) 2460.
[23] J. Baker, The technology–organization–environment framework, Information Systems Theory: Explaining and Predicting Our Digital Society, Vol. 1 (2011) 231–245.
[24] B. Pudjianto, H. Zo, A. P. Ciganek, J. J. Rho, Determinants of e-government assimilation in indonesia: An empirical investigation using a toe framework, Asia Pacific Journal of Information Systems 21 (2011) 49–80.
[25] H. Gangwar, H. Date, A. Raoot, Review on it adoption: insights from recent technologies, Journal of enterprise information management 27 (2014) 488–502.
[26] K. S. R. Warner, M. Wäger, Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal, Long Range Planning 51 (2018) 326–349.
[27] L. E. Valdez-Juárez, E. A. Ramos-Escobar, O. E. Hernández-Ponce, J. A. Ruiz-Zamora, Digital transformation and innovation, dynamic capabilities to strengthen the financial performance of mexican smes: a sustainable approach, Cogent Business & Management 11 (2024) 2318635.
[28] Organisation for Economic Co-operation and Development (OECD), Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies, 2021.
[29] A. I. Ugochukwu, P. W. Phillips, Open data ownership and sharing: Challenges and opportunities for application of fair principles and a checklist for data managers, Journal of Agriculture and Food Research 16 (2024) 101157.
[30] A.-L. Lamprecht, L. Garcia, M. Kuzak, C. Martinez, R. Arcila, et al., Towards fair principles for research software, Data Science 3 (2020) 37–59.
[31] E. A. Schultes, M. Roos, B. Mons, The fair data principles in practice: Designing a data ecosystem for data reuse in healthcare, Studies in Health Technology and Informatics 270 (2020) 227–231.
[32] R. David, A. Rybina, J.-M. Burel, J.-K. Heriche, P. Audergon, J.-W. Boiten, F. Coppens, S. Crockett, K. Exter, S. Fahrner, et al., "be sustainable": Eosc-life recommendations for implementation of fair principles in life science data handling, The EMBO journal 42 (2023) e115008.
[33] European Commission, A european strategy for data, 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066.
[34] G. Peng, W. S. Gross, R. Edmunds, Crosswalks among stewardship maturity assessment approaches promoting trustworthy fair data and repositories, Scientific Data 9 (2022) 576.
[35] D. Tapscott, A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World, Penguin, London, 2016.
[36] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on blockchain technology?—a systematic review, PLOS ONE 11 (2016) e0163477.
[37] G. M. Jonathan, Blockchain-powered decentralisation: A new era of public governance, in: Work-

shop on Advancing Enterprise Modelling through Digital Transformation, FAIR Data Management, and Blockchain Integration, AEM 2024, Tools and Demos, PoEM-Companion, Stockholm, Sweden, December 3-5, 2024, volume 3855, CEUR-WS, 2024.
[38] Y. Li, T. Chen, Blockchain empowers supply chains: challenges, opportunities and prospects, Nankai business review international 14 (2023) 230–248.
[39] S. Makridakis, A. Polemitis, G. Giaglis, S. Louca, Blockchain: Current achievements, future prospects/challenges and its combination with ai, 2017.
[40] G. M. Jonathan, Charting the crossroads of digital sovereignty and digital transformation, in: International Conference on Electronic Government and the Information Systems Perspective, Springer, 2025, pp. 57–71.
[41] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, P. Rimba, A taxonomy of blockchain-based systems for architecture design, in: 2017 IEEE international conference on software architecture (ICSA), IEEE, 2017, pp. 243–252.
[42] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, M. Alazab, Blockchain for industry 4.0: A comprehensive review, Ieee Access 8 (2020) 79764–79800.
[43] M. Atzori, Blockchain technology and decentralized governance: Is the state still necessary?, Journal of Governance and Regulation 6 (2017) 45–62.
[44] J. Sengupta, S. Ruj, S. D. Bit, Fairshare: Blockchain enabled fair, accountable and secure data sharing for industrial iot, IEEE Transactions on Network and Service Management 20 (2023) 2929–2941.
[45] T. L. Nguyen, L. Nguyen, T. Hoang, D. Bandara, Q. Wang, Q. Lu, X. Xu, L. Zhu, S. Chen, Blockchain-empowered trustworthy data sharing: Fundamentals, applications, and challenges, ACM Computing Surveys 57 (2025) 1–36.
[46] F. Mendonça, N. Abdennadher, G. D. M. Serugendo, Fair-er data: Proposing a data model for data cooperatives, in: European Conference on Software Architecture, Springer, 2025, pp. 329–336.
[47] S. Tatineni, Blockchain and data science integration for secure and transparent data sharing, International Journal of Advanced Research in Engineering and Technology (IJARET) 10 (2019) 470–480.
[48] A. Jalbani, R. Weerawarna, K. Al-Zubaidi, Enhancing data provenance in ai with blockchain technology: a comprehensive quality model, CSI Transactions on ICT 13 (2025) 213–224.
[49] G. Li, Q. Zhao, Y. Wang, T. Qiu, K. Xie, L. Feng, A blockchain-based decentralized framework for fair data processing, IEEE Transactions on Network Science and Engineering 8 (2021) 2301–2315.
[50] A. Rot, M. Sobińska, M. Hernes, B. Franczyk, Digital transformation of public administration through blockchain technology, in: Towards Industry 4.0—current challenges in information systems, Springer, 2020, pp. 111–126.
[51] U. Frank, Multi-perspective enterprise modeling: foundational concepts, prospects and future research challenges, Software & Systems Modeling 13 (2014) 941–962.
[52] I. Ilin, A. Levina, A. Borremans, S. Kalyazina, Enterprise architecture modeling in digital transformation era, in: Energy management of municipal transportation facilities and transport, Springer, 2019, pp. 124–142.
[53] E. Rustenova, A. Ibyzhanova, N. Akhmetzhanova, G. Talapbayeva, Z. Yerniyazova, A. Aidaraliyeva, Strategic modeling of enterprise business processes for successful digital transformation, Business, Management and Economics Engineering 23 (2025) 148–163.
[54] A. Tsohou, H. Lee, Z. Irani, V. Weerakkody, I. H. Osman, A. L. Anouze, T. Medeni, Proposing a reference process model for the citizen-centric evaluation of e-government services, Transforming Government: People, Process and Policy 7 (2013) 240–255.
[55] G. Walsham, Doing interpretive research, European Journal of Information Systems 15 (2006) 320–330.
[56] H. K. Klein, M. D. Myers, A set of principles for conducting and evaluating interpretive field studies in information systems, MIS Quarterly 23 (1999) 67–93.
[57] R. K. Yin, Case Study Research and Applications: Design and Methods, 6th ed., Sage, Los Angeles, 2018.