

Organizational Implementation Challenges of Artificial Intelligence and Blockchain:

A Systematic Literature Review

Oliver T. J. de Bruin

Supervisor: Leighann Kimble

Program: IBA – Digital Business & Innovation

Faculty: School of Business and Economics, Vrije Universiteit Amsterdam

Word count: 8369 words (excluding references and appendices)

Date: 30 January 2026

ABSTRACT

This thesis investigates organizational implementation challenges associated with Artificial Intelligence (AI) and Blockchain and examines how interaction or complementarity between these technologies is addressed and evidenced in the academic literature.

Although AI and Blockchain are frequently presented as complementary enablers of digital transformation, existing research primarily demonstrates their complementarity with other technologies and organizational assets, while providing limited evidence of strong complementarity between Artificial Intelligence and Blockchain themselves as a combined technological pairing.

To address this gap, the study adopts a systematic literature review (SLR) methodology in line with established review guidelines. A structured search was conducted in Scopus, resulting in a final sample of 140 peer-reviewed journal articles. The selected studies were screened and qualitatively coded across three analytical dimensions focusing on AI-related organizational implementation challenges, Blockchain-related organizational implementation challenges, and evidence of interaction or complementarity between Artificial Intelligence and Blockchain. The findings show that both technologies face substantial organizational barriers.

AI implementation is primarily constrained by data quality dependency, limited transparency and trust, ethical risks, accountability challenges, and regulatory uncertainty.

Blockchain implementation is mainly hindered by scalability and performance limitations, interoperability and system integration challenges, governance complexity, and regulatory uncertainty. While the joint use of AI and Blockchain is frequently discussed, the literature provides limited empirical evidence of strong interaction or organizational complementarity. Most studies describe parallel co-usage or partial technical complementarity, while deeper organizational or governance-level interdependence remains rare and context-dependent.

Overall, the study concludes that the organizational value of AI and Blockchain is constrained less by technological potential than by governance feasibility. Effective adoption therefore requires clear accountability structures, regulatory awareness, and integration capabilities rather than assumptions of inherent technological synergy.

By systematically synthesizing and comparing implementation challenges across both technologies, this study clarifies when combined adoption increases governance complexity rather than generating complementary value.

CHAPTER 1 – INTRODUCTION	3
1.1 Background and Motivation.....	3
1.2 Problem Statement and Research Gap	3
1.3 Research Question.....	4
1.4 Research Design.....	5
1.5 Theoretical, Practical, and International Relevance.....	5
1.6 Structure of the Thesis	6
CHAPTER 2 – METHODS.....	6
2.1 Research Design.....	7
2.2 Database Selection	7
2.3 Search Strategy.....	7
2.4 Inclusion and Exclusion Criteria	9
2.5 Screening Procedure.....	9
2.6 Coding Strategy.....	10
2.7 Reliability and Validity	11
CHAPTER 3 – SYSTEMATIC LITERATURE REVIEW.....	12
3.1 Organizational Implementation Challenges of Artificial Intelligence	12
3.2 Organizational implementation challenges of Blockchain.....	16
3.3 Extent of Interaction or Complementarity Between Artificial Intelligence and Blockchain	18
3.4 Concluding synthesis in relation to the research question	21
CHAPTER 4 – DISCUSSION & CONCLUSION	22
4.1 Re-addressing the research question	22
4.2 Theoretical implications	23
4.3 Practical implications	25
4.4 Limitations and directions for future research	26
4.5 Conclusion.....	26
References	27
Appendix A – Article Memos	30
Appendix B: Coding Overview Table.....	37

CHAPTER 1 – INTRODUCTION

1.1 Background and Motivation

Artificial Intelligence (AI) and Blockchain have emerged as two of the most influential technologies shaping digital transformation and business innovation (Brynjolfsson & McAfee, 2017; Verhoef et al., 2021). AI enables organizations to automate decision making, enhance predictive capabilities, and optimize operational efficiency through data driven algorithms and learning systems (Brynjolfsson & McAfee, 2017; Shrestha et al., 2019). Blockchain provides technological mechanisms for decentralized coordination, tamper resistant data storage, and enhanced transparency across organizational and interorganizational processes (Tapscott & Tapscott, 2018; Casino et al., 2019).

Rather than being adopted in isolation, digital transformation is increasingly characterized by the concurrent deployment of multiple digital technologies whose organizational implications emerge through interaction rather than standalone use (Yoo et al., 2012; Vial, 2019). AI and Blockchain increasingly underpin digital business models, platform ecosystems, and complex value networks that span organizational and national boundaries (Veit et al., 2014; Nambisan et al., 2017; Verhoef et al., 2021).

Despite their strategic relevance, organizations face substantial challenges when implementing these technologies. AI adoption raises organizational and governance concerns related to algorithmic bias, explainability, data quality dependency, accountability, and the establishment of trust in automated decision systems (Rahwan et al., 2019; Shneiderman, 2020). Blockchain adoption is constrained by scalability and performance limitations, interoperability challenges, regulatory uncertainty, and architectural trade offs such as on chain versus off chain data storage and computation (Treiblmaier, 2018; Xu et al., 2016).

Although AI and Blockchain are frequently discussed as complementary enablers of digital transformation, academic research predominantly examines these technologies in isolation or treats them instrumentally as discrete technological solutions (Vial, 2019; Verhoef et al., 2021). As a result, existing research provides limited insight into how their interaction may shape organizational implementation challenges when both technologies are adopted concurrently within the same transformation trajectory.

1.2 Problem Statement and Research Gap

Research on the organizational implementation of Artificial Intelligence and Blockchain has expanded rapidly in recent years. The AI literature consistently highlights challenges related to data quality dependency, explainability, ethical risks, algorithmic bias, accountability, and governance structures required to oversee automated decision making (Rahwan et al., 2019; Shneiderman, 2020). Similarly, Blockchain research emphasizes organizational barriers including governance complexity in decentralized systems, scalability constraints, interoperability with legacy infrastructures, and regulatory uncertainty across jurisdictions (Treiblmaier, 2018; Xu et al., 2016).

Despite the richness of these research streams, studies on AI and Blockchain largely remain technology specific and are not designed to examine how multiple advanced digital technologies interact within the same organizational context (Yoo et al., 2012; Vial, 2019).

A limited number of conceptual and exploratory studies suggest potential points of interaction or partial complementarities between AI and Blockchain, such as Blockchain supported transparency and auditability in AI systems or AI driven optimization of Blockchain performance (Casino et al., 2019; Zhang et al., 2021). However, these insights remain fragmented and lack systematic synthesis across organizational and business settings.

As a result, it remains unclear whether the academic literature provides consistent evidence of interaction or complementarity between AI and Blockchain at the organizational level. Existing studies do not consolidate AI related and Blockchain related implementation challenges, nor do they systematically assess whether these challenges reinforce, mitigate, or remain independent when both technologies are implemented jointly.

From a theoretical perspective, this fragmentation reflects a deeper limitation. Existing digital transformation and technology adoption theories predominantly conceptualize technologies as independent drivers of organizational change. While such perspectives are well suited to explain technology specific implementation challenges, they provide limited explanatory power when multiple advanced technologies are adopted simultaneously within the same organizational context. Organizational outcomes increasingly emerge from configurations of interdependent technologies rather than from isolated technological investments.

Without an explicit focus on complementarities, it remains theoretically unclear whether organizational challenges observed in joint adoption contexts stem from individual technologies or from their interaction. Consequently, existing theory cannot adequately explain whether the simultaneous adoption of AI and Blockchain leads to reinforcement, tradeoffs, or unintended amplification of governance, accountability, and coordination challenges. This limitation constrains both theoretical integration across research streams and the development of coherent managerial guidance for organizations implementing multiple advanced digital technologies within the same transformation trajectory.

1.3 Research Question

What organizational implementation challenges associated with Artificial Intelligence and Blockchain are reported in the literature, and how does the literature indicate interaction or complementarity between these technologies?

1.4 Research Design

To address this research question, this thesis adopts a Systematic Literature Review methodology. An SLR is particularly appropriate given the fragmented nature of existing research on Artificial Intelligence and Blockchain, where studies are dispersed across multiple domains and primarily focus on technology specific implementation challenges rather than their combined organizational implications.

By applying a structured, transparent, and replicable review protocol, the SLR enables a systematic synthesis of prior academic work without presupposing interaction or complementarity between the two technologies. This approach allows the study to consolidate organizational implementation challenges associated with AI and Blockchain and to assess whether and how the literature documents interaction between them in organizational and business contexts.

The review follows established methodological guidelines for systematic literature reviews, including predefined search terms, explicit inclusion and exclusion criteria, and a multi stage screening process. Peer reviewed academic sources are systematically identified, screened, and qualitatively coded to ensure methodological rigor and minimize selection bias. The full methodological procedure is detailed in Chapter 2.

1.5 Theoretical, Practical, and International Relevance

Theoretical relevance:

From a theoretical perspective, this study is grounded in the complementarity theory, which posits that the organizational value and implications of technologies depend on how they interact with other technologies, organizational structures, and governance mechanisms rather than on isolated adoption (Milgrom & Roberts, 1995; Brynjolfsson & Milgrom, 2013). Complementarity theory emphasizes that organizational outcomes emerge from configurations of interdependent elements, where technologies may mutually reinforce, constrain, or condition each other.

Applying a complementarities-oriented lens is theoretically necessary to address the limitations of existing digital transformation theories that predominantly examine single technologies in isolation. By systematically synthesizing literature on AI and Blockchain implementation challenges, this study extends complementarity theory to a multi technology organizational context. It examines whether governance, accountability, trust, and coordination challenges reinforce, mitigate, or remain independent when both technologies are implemented simultaneously, without presupposing synergistic outcomes (Teece, 2018; Vial, 2019).

Practical relevance:

From a practical perspective, organizations face significant uncertainty when adopting AI and Blockchain as part of digital transformation initiatives. AI driven systems raise concerns related to explainability, fairness, accountability, and trust in automated decision making, while Blockchain implementations confront challenges associated with coordination, compliance, scalability, and integration with existing organizational infrastructures (Shneiderman, 2020; Xu et al., 2016). By synthesizing reported implementation challenges and assessing how the literature indicates interaction or complementarity between the two technologies, this thesis provides a structured basis for managerial decision making in contexts where organizations must govern multiple advanced digital technologies concurrently.

International relevance:

Both Artificial Intelligence and Blockchain are frequently implemented in international and cross organizational settings, including platform ecosystems, global supply chains, and public service networks. Blockchain applications are explicitly associated with international coordination and provenance challenges, while AI governance concerns similarly extend across jurisdictions characterized by heterogeneous regulatory regimes and accountability standards (Treiblmaier, 2018; Xu et al., 2016). Consequently, the insights generated by this study are relevant for organizations operating in international business environments marked by complex coordination demands and fragmented institutional frameworks.

Societal relevance:

The societal relevance of this study follows from the increasing influence of AI and Blockchain on decision making and coordination in domains with significant public impact. AI based systems affect access to services, resource allocation, and risk assessment, increasing the importance of transparency, fairness, and accountable governance (Rahwan et al., 2019; Shneiderman, 2020). Blockchain based infrastructures influence transparency, auditability, and responsibility allocation across organizational boundaries, particularly in cross border contexts where governance arrangements are complex (Treiblmaier, 2018). By synthesizing implementation challenges and examining whether interaction between the technologies is evidenced in the literature, this study supports more realistic and governable adoption strategies.

1.6 Structure of the Thesis

The remainder of this thesis is structured as follows. Chapter 2 outlines the methodological framework of the systematic literature review, including database selection, search strategy, inclusion and exclusion criteria, and screening and coding procedures. Chapter 3 presents the results of the review, addressing organizational implementation challenges related to Artificial Intelligence and Blockchain and examining how the literature indicates interaction or complementarity between the two technologies. Chapter 4 discusses the theoretical and managerial implications of the findings, reflects on the study's limitations, and concludes with directions for future research.

CHAPTER 2 – METHODS

2.1 Research Design

This study employs a Systematic Literature Review (SLR) to investigate organizational implementation challenges associated with AI and Blockchain and to assess whether the literature documents any interaction or complementarity between them. An SLR is appropriate because it provides a transparent and rigorous approach to synthesizing scientific knowledge across multiple disciplines (Tranfield et al., 2003; Snyder, 2019). The unit of analysis is the peer-reviewed journal article, written in English and positioned within the domains of business, management, economics, decision sciences, and computer science.

2.2 Database Selection

The primary database used for the literature search is Scopus, due to its extensive coverage of high-quality international journals, strong indexing standards, broad disciplinary representation, and advanced TITLE-ABS-KEY search functionality. To ensure completeness, forward- and backward-snowballing techniques were applied during the full-text phase.

2.3 Search Strategy

2.3.1 Conceptual Basis

The search strategy was developed around three core conceptual pillars, reflecting both the technological scope and the organizational focus of this study. These pillars comprise **Artificial Intelligence (AI)**, **Blockchain and Distributed Ledger Technologies (DLT)**, and **digital business models and digital transformation**.

The first pillar, Artificial Intelligence, captures a broad range of data-driven and algorithmic decision-making technologies, including machine learning and automated decision systems, which are frequently associated with organizational challenges related to transparency, accountability, trust, and governance.

The second pillar, Blockchain and Distributed Ledger Technologies, encompasses decentralized infrastructures such as distributed ledgers, smart contracts, and token-based systems, which introduce distinct organizational and governance challenges related to coordination, scalability, interoperability, and regulatory compliance.

The third pillar, digital business models and digital transformation, was included to ensure that the literature search captured studies examining AI and Blockchain within an explicit organizational, managerial, and business context. This pillar served to exclude purely technical or engineering-oriented studies and to focus the review on organizational implementation challenges rather than isolated technological performance. Complementarity theory was intentionally not included as a search term, in line with established systematic literature review practices, to avoid excessively narrowing the search results. Instead, complementarity was applied as an analytical lens during the coding and synthesis phases.

This approach enabled an open and inductive assessment of whether and how the reviewed literature provides evidence of interaction or complementarity between AI and Blockchain at the organizational level.

Together, these conceptual pillars directly informed the construction of the search string and guided the subsequent coding framework, which distinguishes between AI-related implementation challenges, Blockchain-related implementation challenges, and instances of interaction or complementarity between the two technologies.

2.3.2 Executed Scopus Search String

The following Boolean query was executed at the TITLE-ABS-KEY level in Scopus:

```
(TITLE-ABS-KEY("artificial intelligence" OR "machine learning"  
OR "algorithmic system*" OR "algorithmic decision*" OR "AI-driven" OR "automated decision*"))  
AND  
(TITLE-ABS-KEY("Blockchain" OR "distributed ledger"  
OR "DLT" OR "Web3" OR "tokenization"  
OR "smart contract*" OR "DAO"))  
AND  
(TITLE-ABS-KEY("digital business model*" OR "digital transformation"  
OR "platform*" OR "digital innovation"))
```

The search was executed in December 2025.

2.3.3 Applied Filters

After running the query, the following Scopus filters were applied:

- Document type: Article, Review
 - Language: English
 - Subject areas:
 - Business, Management & Accounting
 - Economics, Econometrics & Finance
 - Computer Science
 - Decision Sciences
- Publication years: 2000–2025

These subject areas were selected to align with the organizational and managerial focus of the study, while still capturing relevant interdisciplinary research on Artificial Intelligence and Blockchain.

The lower bound was set at 2000 to capture early conceptual work on digital transformation, while the upper bound reflects the most recent available literature available at the time of the search. After applying these filters, **894 articles** remained for initial screening.

2.4 Inclusion and Exclusion Criteria

Inclusion Criteria:

- Articles were included when they:
- Were peer-reviewed journal articles or reviews
- Were written in English
- Examined AI, Blockchain, or both within an organizational or business context
- Addressed digital business models, digital transformation, or managerial/organizational implications
- Were published between 2000 and 2025
- Fell within the selected subject areas

Exclusion Criteria:

- Articles were excluded when they:
 - Had a purely technical, engineering-only, or cryptographic focus without business relevance
 - Were conference papers, book chapters, dissertations, or non-peer-reviewed manuscripts
 - Did not address organizational aspects of AI or Blockchain
 - Did not provide conceptual or empirical insights relevant to digital business models
 - Did not provide accessible full-text
-

2.5 Screening Procedure

Figure 1 presents the PRISMA 2020 flow diagram summarizing the identification, screening, eligibility assessment, and inclusion of studies in this systematic literature review. Following the predefined search strategy and applied filters, 894 records were identified through Scopus.

All records were screened at the title and abstract level, resulting in the exclusion of 607 records due to insufficient relevance to the research scope. Subsequently, 287 reports were sought for full text retrieval, of which 12 could not be obtained, leaving 275 reports assessed for eligibility. During the full text assessment, 135 reports were excluded due to a purely technical focus, cryptography only orientation, insufficient relevance to organizational or business contexts, or other conceptual misalignment with the study objectives, as detailed in Figure 1.

The final sample consisted of 140 studies included in the qualitative synthesis. The screening and selection process followed the PRISMA 2020 guidelines, ensuring transparency, consistency, and methodological rigor (Page et al., 2021). To support replicability and auditability, Appendix A documents the screening and coding memos used throughout the review process. AI tools were used exclusively for language refinement and reference formatting and did not influence analytical decisions.

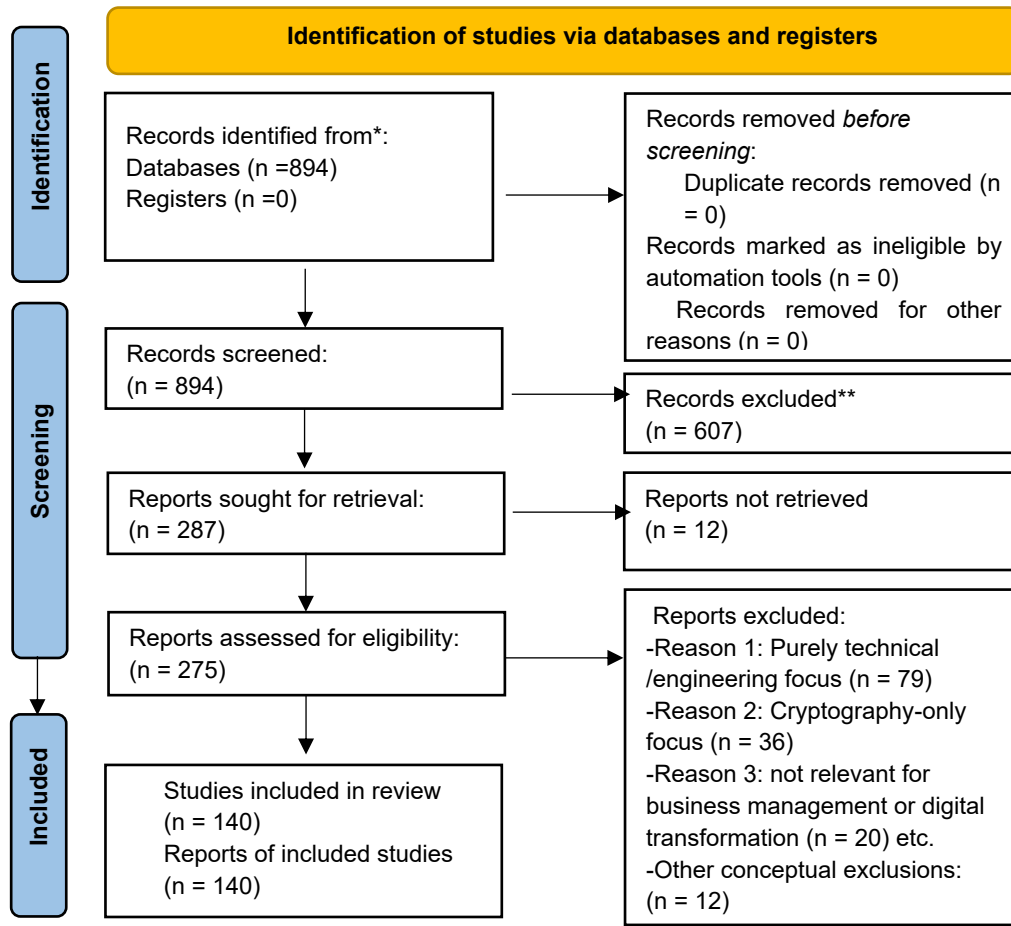


Figure 1 PRISMA 2020 flow diagram of the study selection process.

2.6 Coding Strategy

A qualitative coding strategy was employed to structure and synthesize the final dataset resulting from the systematic literature review. The qualitative coding process followed an inductive thematic analysis approach informed by the principles outlined by Braun and Clarke (2006). This approach was selected because it enables systematic identification, comparison, and synthesis of patterns across heterogeneous qualitative studies without imposing predefined theoretical categories.

The coding strategy combined deductive and inductive elements, consistent with established guidelines for qualitative synthesis in management and information systems research (Tranfield et al., 2003; Snyder, 2019). The initial coding framework was developed deductively based on the research question and the theoretical foundation of the study, particularly complementarity theory and prior literature on organizational implementation challenges associated with Artificial Intelligence and Blockchain. Based on this framework, three analytical dimensions guided the coding process.

The first dimension focused on Artificial Intelligence related organizational challenges, including data quality dependency, explainability challenges, algorithmic bias, ethical concerns, trust in automated decision making, governance constraints, and organizational adoption barriers.

The second dimension addressed Blockchain related organizational challenges, such as scalability limitations, interoperability constraints, governance complexity, regulatory uncertainty, integration with legacy systems, and operational immaturity.

The third analytical dimension examined evidence of interaction or complementarity between Artificial Intelligence and Blockchain. Guided by complementarity theory, this dimension captured explicit or implicit indications of interaction, including reinforcing or mitigating effects, interdependencies, alignment between technologies, complementary capabilities, and joint value creation in digital business models. Studies describing parallel adoption without interaction were coded separately to distinguish absence of complementarity from interaction effects.

Consistent with Braun and Clarke (2006), the coding process involved familiarization with the data, initial code generation, iterative refinement of codes, and aggregation of codes into higher level analytical themes. Subcategories were identified inductively through iterative comparison across studies, allowing the coding structure to remain flexible while ensuring consistency across the dataset. Coding was conducted manually to ensure close engagement with the content. Analytical memos were maintained throughout the coding and synthesis process to document coding decisions and emerging patterns.

2.7 Reliability and Validity

Reliability and validity were addressed through a combination of transparent review procedures, systematic documentation, and established qualitative analysis principles. Reliability was strengthened through a predefined and replicable search strategy, clearly specified inclusion and exclusion criteria, and a multi stage screening process following PRISMA guidelines (Tranfield et al., 2003; Page et al., 2021).

Analytical rigor was supported through iterative comparison, reflexive memoing, and systematic documentation of coding decisions, in line with established qualitative analysis principles (Miles et al., 2014). Analytical memos provided an explicit audit trail of interpretive decisions and category development and are included in Appendix A.

Validity was supported through several complementary strategies. The use of a multidisciplinary database and snowballing techniques increased coverage across academic domains, reducing disciplinary bias.

The coding framework was theoretically informed but not imposed deductively, allowing interaction, tension, or independence between Artificial Intelligence and Blockchain to emerge inductively from the literature (Braun & Clarke, 2006). Construct validity was further enhanced by systematically comparing organizational challenges across Artificial Intelligence focused studies, Blockchain focused studies, and studies addressing both technologies.

The qualitative synthesis was based on a final sample of 140 peer reviewed studies. Within this sample, a focused subset of 29 studies explicitly addressed organizational challenges and interaction or complementarity between Artificial Intelligence and Blockchain.

These studies form the analytical core of the synthesis presented in Chapters 3 and 4 and are documented in Appendix B.

CHAPTER 3 – SYSTEMATIC LITERATURE REVIEW

This chapter presents the results of the systematic literature review and synthesizes the findings in relation to the research question. The review is structured around three analytical dimensions derived from the coding process.

Section 3.1 examines organizational implementation challenges related to Artificial Intelligence, Section 3.2 addresses organizational implementation challenges related to Blockchain, and Section 3.3 explores interaction and complementarity between the two technologies, distinguishing between co-usage and functional or organizational interdependence.

Together, these sections provide a structured synthesis of existing research and form the empirical basis for the discussion in Chapter 4. An overview of the coding of individual studies across these dimensions is provided in Appendix B. While the full sample of 140 studies informed the analyses in Sections 3.1 and 3.2, a focused subset of 29 studies explicitly addressing AI–Blockchain interaction formed the basis for Section 3.3.

Consistent with complementarity theory, interaction is understood as a relationship in which the organizational implications of one technology are conditioned by the presence, configuration, or governance of the other technology, rather than being independent. Complementarity in this review does not imply automatic synergy.

Instead, it is treated as an empirical pattern that may involve reinforcing effects, mitigating effects, or governance and coordination tradeoffs that emerge when technologies are combined within the same organizational trajectory (Milgrom & Roberts, 1995; Brynjolfsson & Milgrom, 2013; Teece, 2018).

Table 3.1 Analytical dimensions and key organizational challenge categories structuring the findings in Sections 3.1–3.3

Analytical dimension	Key categories / themes identified
AI-related organizational challenges	Data quality and dependency; explainability; bias and ethics; governance and accountability; trust in automation
Blockchain-related organizational challenges	Scalability; interoperability; governance complexity; regulatory uncertainty; integration with legacy systems
Interaction / complementarity	Parallel co-usage; functional complementarity; governance tensions; organizational interdependence

3.1 Organizational Implementation Challenges of Artificial Intelligence

The reviewed literature identifies a broad set of organizational implementation challenges associated with the adoption and deployment of Artificial Intelligence. Across domains and application contexts, AI implementation is rarely portrayed as a purely technical endeavor. Instead, the literature consistently emphasizes that organizational factors, governance arrangements, and institutional conditions play a decisive role in determining whether AI systems can be successfully integrated into organizational processes. This section synthesizes the key organizational implementation challenges of AI reported in the literature.

3.1.1 Data quality and data dependency

The reviewed literature identifies data quality and data dependency as central organizational challenges in the implementation of Artificial Intelligence. Across application contexts, AI systems are shown to depend heavily on the availability of accurate, reliable, and representative data, with limitations in data quality directly undermining system performance and reliability regardless of algorithmic sophistication.

A recurring theme concerns organizational difficulties arising from fragmented data landscapes and limited data integration. Data is frequently distributed across organizational units, partners, or external sources, complicating aggregation, validation, and consistent use for AI training and deployment. In decentralized and multi-actor settings, such fragmentation reduces visibility into data provenance and constrains organizations' ability to ensure data consistency across contributors (e.g., Djolev et al., 2024; Alghamdi et al., 2022; Otoum et al., 2021).

Beyond technical constraints, data quality challenges are widely framed as governance-related issues. The literature highlights ambiguity regarding responsibility for data contribution, maintenance, and quality assurance, particularly in collaborative environments such as federated learning, healthcare systems, and distributed data-sharing arrangements. Insufficient governance mechanisms are shown to exacerbate concerns related to data reliability, transparency, and fairness, as organizations lack effective means to verify data quality across participating entities (e.g., Peyvandi et al., 2022; Zerka et al., 2020; Escorcia-Gutierrez et al., 2024; Witowski et al., 2021).

Studies on Blockchain-enabled crowdsourcing and collaborative data platforms further emphasize that maintaining data quality in distributed environments depends on organizational coordination mechanisms, including incentive design, validation procedures, and quality control processes (e.g., Xu et al., 2016; Liang et al., 2024; Wang et al., 2021).

Taken together, the literature suggests that data quality constitutes an organizational outcome shaped by governance arrangements and coordination structures rather than a purely technical input. As a result, data dependency emerges as a foundational organizational constraint on AI implementation.

3.1.2 Explainability, transparency, and trust

The reviewed literature identifies transparency and trust as critical organizational challenges in the implementation of Artificial Intelligence. Across application domains, AI systems are frequently described as difficult to scrutinize or audit, which complicates their acceptance within organizational decision-making processes, particularly in regulated, safety critical, or high stakes contexts.

A recurring concern relates to the relationship between transparency mechanisms and organizational trust. Studies examining Blockchain-enabled federated learning, smart contracts, and AI-driven platforms emphasize that trust in AI systems is closely linked to the presence of auditable, traceable, and verifiable governance mechanisms rather than model-level interpretability alone (e.g., Biswas et al., 2024; Djolev et al., 2024; Oktian et al., 2022; Wahrstätter et al., 2024).

In such contexts, auditable records and verifiable execution histories support organizational confidence when AI decisions must be reviewed, validated, or contested.

The literature further indicates that transparency challenges extend beyond technical system design to organizational accountability structures. Unclear attribution of responsibility for AI-driven outcomes is shown to undermine trust and increase perceived organizational risk, particularly in decentralized system architectures. When accountability arrangements are insufficiently defined, organizations face difficulties in assigning responsibility for errors, biases, or unintended consequences, which constrains large scale adoption (e.g., Haddad et al., 2022; Truong et al., 2024; Yang et al., 2024).

In response, several technical studies explore the integration of Blockchain-based mechanisms to enhance transparency through immutable logs, auditable decision trails, and verifiable execution records (e.g., Kumar et al., 2024; Salim et al., 2024; Rathod et al., 2023). However, the literature consistently notes that such technical solutions do not resolve underlying organizational governance and accountability challenges and may introduce additional coordination and oversight requirements.

Overall, transparency and trust emerge as organizational barriers shaped by governance arrangements and responsibility allocation rather than solely technical system properties.

3.1.3 Ethical concerns, algorithmic bias, and accountability

The reviewed literature identifies ethical concerns and algorithmic bias as persistent organizational challenges in the implementation of Artificial Intelligence. Across domains, AI systems are associated with risks related to fairness, discrimination, and unintended consequences, particularly when algorithmic outputs affect individuals or groups within complex socio technical systems.

A central theme concerns algorithmic bias arising from data quality limitations and data heterogeneity in distributed learning environments. Studies on hybrid AI and Blockchain systems indicate that biased, incomplete, or unrepresentative data contributions can result in systematically skewed outcomes that organizations may find difficult to detect and correct once models are deployed (e.g., Zerka et al., 2020; Wang et al., 2021; Alibašić, 2025).

These risks are especially salient in contexts such as healthcare, supply chains, and platform ecosystems, where AI driven decisions carry significant operational and societal implications.

Beyond bias, the literature highlights ethical challenges related to accountability and responsibility allocation. The integration of AI into decentralized or Blockchain based environments complicates traditional accountability structures, as decision making processes are distributed across multiple technical components and organizational actors.

This diffusion of responsibility makes it difficult to assign accountability for errors, biases, or unintended outcomes and is frequently identified as a barrier to large scale deployment (e.g., Truong et al., 2024; Yang et al., 2024; Alibašić, 2025).

While some studies propose Blockchain based mechanisms to enhance ethical oversight through improved traceability, audibility, and data integrity, the literature cautions that technical safeguards alone are insufficient.

Ethical risks persist unless organizations complement technical measures with clearly defined governance structures, ethical guidelines, and oversight mechanisms (e.g., Zerka et al., 2020; Kumar et al., 2024; Haddad et al., 2022). Overall, ethical concerns, algorithmic bias, and accountability challenges emerge as fundamental organizational barriers to AI implementation.

3.1.4 Governance, regulation, and compliance

The reviewed literature identifies governance, regulation, and compliance as central organizational challenges in the implementation of Artificial Intelligence. Across sectors, studies indicate that AI development and deployment frequently outpace the establishment of clearly articulated governance arrangements, leaving organizations uncertain about how to oversee and legitimize AI-driven systems within existing structures.

A recurring theme concerns the absence of clearly defined governance structures, particularly in contexts where AI is combined with decentralized or Blockchain-based infrastructures. Organizations experience difficulties in assigning roles, responsibilities, and decision rights when control is distributed across technical components, organizational units, or external stakeholders, which discourages large scale implementation (e.g., Alibašić, 2025; Khaskheli et al., 2025; Wu et al., 2025).

Regulatory uncertainty represents an additional organizational constraint. The literature highlights that organizations often operate within fragmented or evolving regulatory environments governing AI use, data protection, and automated decision making.

Such ambiguity complicates compliance efforts, increases perceived legal and reputational risks, and may lead organizations to postpone adoption or restrict deployment to lower risk applications (e.g., Wirata et al., 2025; Yang et al., 2024).

Compliance challenges are further intensified in cross sector and cross jurisdictional contexts, where AI systems must adhere to heterogeneous legal, ethical, and sector specific standards. This generates additional coordination, monitoring, and reporting burdens, particularly in domains such as supply chains, smart cities, and platform-based ecosystems (e.g., Sunmola et al., 2025; Lukić et al., 2025).

The literature also notes tensions between innovation and control. While governance mechanisms are necessary to ensure legitimacy and accountability, overly rigid frameworks may constrain experimentation and slow innovation. Organizations are therefore portrayed as balancing the need for effective governance with the flexibility required for technological adaptation (e.g., Fasano et al., 2025; Wang et al., 2021).

Overall, governance, regulation, and compliance challenges emerge as core organizational constraints shaping AI implementation.

3.2 Organizational implementation challenges of Blockchain

3.2.1 Scalability and performance limitations

The reviewed literature consistently identifies scalability and performance limitations as central organizational challenges in Blockchain implementation. Across application domains, Blockchain-based systems face constraints related to transaction throughput, processing latency, and computational overhead, limiting their suitability for large scale organizational deployment.

A recurring theme concerns the tradeoff between decentralization and system performance. Consensus mechanisms and distributed validation processes introduce delays that intensify as network size and transaction volume increase (e.g., Wang et al., 2024; Rajmohan et al., 2024).

These limitations are particularly problematic in contexts requiring timely data processing or continuous data exchange, such as Internet of Things environments and data intensive applications (e.g., Escorcia-Gutierrez et al., 2024; Hemdan & Mahmoud, 2025).

From an organizational perspective, scalability constraints translate into architectural and governance tradeoffs. Organizations frequently adopt permissioned Blockchains, hybrid architectures, or off chain computation to mitigate performance bottlenecks (e.g., Wang et al., 2024; Tekchandani et al., 2025). While these solutions improve efficiency, they increase system complexity, coordination requirements, and governance overhead.

Several studies further note that high computational demands raise operational costs and barriers to adoption, particularly for resource constrained organizations, resulting in Blockchain initiatives remaining limited to pilots or domain specific deployments (e.g., Rajmohan et al., 2024; Escorcia-Gutierrez et al., 2024).

Overall, scalability and performance limitations emerge as central organizational constraints shaping Blockchain adoption decisions.

3.2.2 Interoperability and System Integration Challenges

The reviewed literature identifies interoperability and system integration as persistent organizational challenges in Blockchain implementation. Although often presented as an independent infrastructural layer, empirical studies show that Blockchain deployments typically require integration with existing digital systems and complementary technologies.

A recurring issue concerns integration with heterogeneous technical environments. Blockchain solutions must interface with external data sources, application layers, and legacy systems that rely on differing data structures and operational assumptions, increasing architectural complexity and implementation effort (e.g., Rehman et al., 2024; Escorcia-Gutierrez et al., 2024).

Interoperability challenges are particularly pronounced in multi organizational and cross domain settings. Studies in healthcare, smart infrastructure, and supply chains report difficulties coordinating data flows across organizations with distinct systems and practices, compounded by the absence of widely adopted interoperability standards (e.g., Hemdan & Mahmoud, 2025; Lukić et al., 2025).

Beyond technical compatibility, interoperability also entails organizational coordination and governance alignment. Insufficient integration governance is associated with fragmented implementations and reduced organizational impact in consortium-based deployments (e.g., Lukić et al., 2025; Wang et al., 2024).

Overall, interoperability and integration challenges constitute a central organizational constraint, requiring both technical solutions and sustained governance coordination.

3.2.3 Governance Complexity

The reviewed literature consistently identifies governance complexity as a central organizational challenge in Blockchain implementation. Blockchain-based architectures feature decentralized control, shared decision making, and multi stakeholder participation, fundamentally altering governance arrangements within and across organizations.

A key challenge concerns the allocation of roles, responsibilities, and accountability. Authority is distributed among validators, consortium members, and platform operators, complicating responsibility for system maintenance, rule enforcement, and risk management (e.g., Rahaman et al., 2024; Wu et al., 2025). This shift toward protocol-based coordination increases managerial oversight complexity and reduces decision making flexibility.

Governance challenges are amplified in consortium based and cross organizational settings, where divergent objectives, unequal influence, and misaligned incentives hinder collective decision making. Empirical studies link insufficiently specified governance arrangements to coordination failures and constrained adoption (e.g., Lukić et al., 2025; Wirata et al., 2022).

Regulatory uncertainty adds an additional layer of complexity, as Blockchain systems often operate across jurisdictions with evolving legal frameworks, creating ambiguity regarding compliance, data governance, and liability (e.g., Khaskheli et al., 2023; Yang et al., 2024). Overall, governance complexity emerges as a fundamentally organizational challenge requiring adaptation of governance structures, accountability mechanisms, and coordination practices.

3.2.4 Regulatory uncertainty and compliance challenges

While regulatory compliance is discussed as an integrated governance concern in the Artificial Intelligence literature, Blockchain-related studies more frequently treat regulatory uncertainty as a distinct organizational constraint due to the technology's decentralized and cross-jurisdictional nature.

The reviewed literature consistently identifies regulatory uncertainty as a major organizational challenge in the implementation of Blockchain technology.

Unlike conventional information systems that operate within relatively clear organizational and legal boundaries, Blockchain-based systems often span multiple organizations, sectors, and jurisdictions, complicating alignment with existing regulatory arrangements.

A central issue concerns the tension between core Blockchain characteristics such as decentralization, immutability, and distributed governance and established regulatory requirements related to accountability, data protection, and legal responsibility. Several studies indicate that prevailing regulatory frameworks are largely designed around centralized control structures, creating difficulties when applied to decentralized Blockchain architectures (e.g., Khaskheli et al., 2023; Wirata et al., 2022).

Compliance challenges are particularly pronounced in public sector, consortium based, and cross organizational contexts. Research on smart cities, supply chain networks, and digital public services shows that Blockchain initiatives often must comply simultaneously with multiple regulatory regimes, including transparency obligations, data protection requirements, and sector specific rules. This regulatory multiplicity increases organizational complexity and slows implementation processes (e.g., Lukić et al., 2025; Wu et al., 2025).

The literature further highlights regulatory fragmentation across jurisdictions as a constraint on scalable adoption. Differences in national legal frameworks governing digital records, smart contracts, and data governance limit interoperability and create uncertainty regarding the cross-border validity of Blockchain-based transactions.

As a result, organizations frequently restrict deployments to pilot projects or geographically bounded applications (e.g., Yang et al., 2024; Khaskheli et al., 2023).

Uncertainty surrounding the legal recognition and enforceability of smart contracts constitutes an additional compliance challenge. Although smart contracts are promoted as mechanisms for automating coordination and reducing transaction costs, their legal status remains unevenly defined across jurisdictions. This ambiguity complicates liability allocation and dispute resolution, leading organizations to adopt a cautious approach when applying smart contracts to critical processes (e.g., Wirata et al., 2022; Rahaman et al., 2024).

Overall, regulatory uncertainty and compliance challenges emerge as structural organizational constraints on Blockchain implementation rather than temporary transitional issues. In the absence of clearer regulatory guidance, legal harmonization, and sector specific governance standards, organizations remain hesitant to scale Blockchain-based solutions beyond controlled or experimental settings. Consequently, regulatory uncertainty plays a decisive role in shaping the pace, scope, and organizational configuration of Blockchain adoption.

3.3 Extent of Interaction or Complementarity Between Artificial Intelligence and Blockchain

The reviewed literature presents a nuanced and heterogeneous picture regarding interaction between Artificial Intelligence and Blockchain technologies. While many studies refer to their combined use, the depth and nature of integration vary considerably. To maintain analytical clarity, this section distinguishes three patterns.

First, parallel co usage refers to configurations in which the technologies coexist in the same context but remain largely independent in function and governance.

Second, functional complementarity refers to technical level coupling in which one technology enables or improves processes related to the other.

Third, organizational or governance level interdependence refers to situations in which joint adoption affects accountability, decision rights, or coordination structures beyond technical integration.

3.3.1 Parallel co-usage without deep integration

A substantial portion of the reviewed studies describes AI and Blockchain as being deployed within the same organizational or technological context without deep functional integration. In such configurations, the two technologies serve largely independent purposes and operate in distinct layers of the system architecture.

Blockchain is commonly employed for functions such as data logging, access control, provenance tracking, or coordination, while AI systems perform analytics, prediction, or decision support tasks outside the Blockchain layer.

Several studies indicate that this form of co usage is primarily shaped by practical and technical constraints rather than by deliberate efforts to achieve strong complementarity. Limitations related to computational capacity, latency, and scalability are frequently reported as reasons why AI models are not executed directly on Blockchain infrastructures.

As a result, AI processing is often decoupled from Blockchain-based coordination or control mechanisms, leading to architectures in which the two technologies coexist but remain technically and organizationally distinct (e.g., Djolev et al., 2024; Wahrstätter et al., 2024; Wang et al., 2021). The literature suggests that such parallel co usage is associated with limited organizational transformation.

While these implementations may enhance transparency, traceability, or auditability of data flows related to AI systems, they do not substantially reconfigure governance arrangements, decision making structures, or accountability mechanisms. Accordingly, several studies characterize these configurations as incremental extensions of existing systems rather than as instances of deep technological or organizational complementarity.

3.3.2 Functional complementarity at the technical level

A second stream of literature identifies more substantive forms of interaction in which Artificial Intelligence and Blockchain perform complementary technical functions within a shared system architecture. In these configurations, Blockchain is employed to support trust related functions such as data integrity, auditability, and coordination around AI-related processes, while AI contributes analytical, automation, or optimization capabilities within Blockchain-enabled environments.

Examples frequently discussed in the literature include Blockchain-supported federated learning, AI-enabled smart contracts, and Blockchain-based platforms for managing or exchanging machine learning models.

Studies in these domains indicate that Blockchain can provide verifiable data provenance, immutable audit trails, and decentralized coordination mechanisms that support trustworthy AI deployment in distributed settings (e.g., Biswas et al., 2024; Kumar et al., 2024; Salim et al., 2024; Truong et al., 2024).

Conversely, a smaller subset of studies describes how AI techniques may enhance Blockchain-based systems by supporting functions such as anomaly detection, monitoring, or decision support within Blockchain environments.

These studies suggest that AI can contribute to identifying irregular behavior or supporting adaptive responses in Blockchain networks, without fundamentally altering underlying consensus or governance mechanisms (e.g., Rajawat et al., 2024; Shahbazi & Byun, 2021).

Despite these complementarities, the literature consistently notes that functional integration remains technically and organizationally demanding. Hybrid architectures often require complex coordination between on chain and off chain components, specialized technical expertise, and the development of additional governance mechanisms.

As a result, functional complementarity is most frequently observed in experimental settings, pilot projects, or domain specific applications rather than in mature, enterprise wide deployments.

3.3.3 Organizational and governance-level interdependence

Only a limited subset of the reviewed studies suggests deeper forms of interaction that extend beyond technical complementarity to organizational or governance level interdependence. These studies argue that the combined adoption of AI and Blockchain may influence accountability structures, decision rights, and coordination practices within organizations or inter organizational ecosystems.

Research focusing on ethical governance frameworks, decentralized decision making, and multi stakeholder platforms indicates that Blockchain-enabled transparency and auditability can support organizational oversight of AI systems, particularly in environments characterized by low trust, high complexity, or heightened regulatory scrutiny (e.g., Alibašić, 2025; Yang et al., 2024; Wirata et al., 2025). In these contexts, Blockchain is portrayed as an infrastructural layer that enables distributed control while preserving traceability and accountability over AI-related processes.

However, the literature also emphasizes that such organizational interdependence introduces new tensions and coordination challenges. Decentralized governance arrangements can complicate responsibility allocation, compliance management, and managerial control, especially when AI systems influence outcomes across organizational boundaries. Consequently, several studies caution that organizational complementarity between AI and Blockchain remains fragile and highly context dependent, requiring deliberate governance design, clear role definition, and institutional alignment to be sustained (e.g., Fasano et al., 2025; Wu et al., 2025; Khaskheli et al., 2025).

3.3.4 Synthesis of interaction patterns

Overall, the reviewed literature reveals a clear pattern in how interaction between Artificial Intelligence and Blockchain is conceptualized. Most studies describe parallel co-usage, a smaller subset identifies partial technical complementarity, while only a limited number suggest organizational or governance-level interdependence.

Importantly, complementarity is not uniformly positive in the reviewed studies. Where interaction is observed, it can involve both reinforcing mechanisms and tradeoffs, such as increased auditability coupled with higher coordination and governance overhead.

The nature of interaction between AI and Blockchain appears to be shaped primarily by application context, regulatory conditions, and organizational capabilities rather than by inherent technological synergy alone.

These findings suggest that AI and Blockchain should not be treated as inherently complementary technologies. Instead, their interaction emerges through specific architectural choices, governance arrangements, and strategic objectives.

3.4 Concluding synthesis in relation to the research question

Consequently, the literature reveals a clear gap between conceptual narratives that emphasize AI–Blockchain synergy and empirical evidence documenting fragmented, cautious, and context-dependent forms of integration. This divergence provides an important foundation for the discussion in Chapter 4.

Taken together, the findings of this systematic literature review provide a structured response to the research question concerning organizational implementation challenges associated with Artificial Intelligence and Blockchain and the extent to which the literature indicates interaction or complementarity between these technologies.

Sections 3.1 and 3.2 show that both Artificial Intelligence and Blockchain are associated with substantial organizational implementation challenges, which are largely examined in technology-specific terms.

The AI literature emphasizes data quality dependency, explainability, ethical risks, accountability, and governance uncertainty, indicating that successful AI implementation depends heavily on organizational data governance, trust, and institutional legitimacy.

In contrast, the Blockchain literature focuses primarily on scalability, interoperability, governance complexity, and regulatory uncertainty, highlighting difficulties in deploying decentralized infrastructures within existing organizational and legal frameworks.

Notably, these challenges are predominantly analyzed in isolation. Most studies examine Artificial Intelligence or Blockchain separately, even when both technologies are referenced within the same application domain, resulting in limited insight into how organizations manage their combined implementation as part of shared transformation trajectories.

Section 3.3 further demonstrates that, although joint use is frequently discussed, empirical evidence of strong interaction or structural complementarity remains limited.

Most studies describe parallel co-usage, while a smaller body of literature identifies functional complementarity at the technical level, typically confined to experimental, pilot, or domain-specific contexts.

Only a limited subset of studies suggests deeper forms of interaction at the organizational or governance level, proposing that Blockchain-enabled transparency and auditability may support oversight, accountability, or trust in AI-driven systems, particularly in regulated or multi-actor environments.

At the same time, these studies emphasize that such interdependence introduces additional governance complexity and remains highly context-dependent.

Overall, the findings indicate that Artificial Intelligence and Blockchain should not be regarded as inherently complementary technologies at the organizational level.

Instead, any form of interaction or complementarity emerges through deliberate design choices, governance arrangements, and contextual conditions rather than through automatic technological synergy.

CHAPTER 4 – DISCUSSION & CONCLUSION

4.1 Re-addressing the research question

This thesis addressed the following research question:

What organizational implementation challenges associated with Artificial Intelligence and Blockchain are reported in the literature, and how does the literature indicate interaction or complementarity between these technologies?

The findings presented in Chapter 3 provide a structured response to this research question along three analytical dimensions derived from the coding process. These dimensions concern organizational implementation challenges related to Artificial Intelligence (Section 3.1), organizational implementation challenges related to Blockchain (Section 3.2), and patterns of interaction or complementarity between the two technologies (Section 3.3).

First, the literature on Artificial Intelligence indicates that implementation outcomes are shaped primarily by organizational rather than purely technical factors. As synthesized in Section 3.1, recurring challenges include data quality dependency, limited transparency and trust in AI-driven outcomes, ethical risks and algorithmic bias combined with unclear accountability, and governance, regulatory, and compliance uncertainty.

Together, these findings suggest that successful AI implementation depends heavily on organizational data governance, clearly defined responsibility structures, and institutional legitimacy, rather than on advances in algorithmic design alone (Brynjolfsson & McAfee, 2017; Rahwan et al., 2019; Shneiderman, 2020).

Second, the literature on Blockchain identifies a distinct but equally substantial set of organizational implementation challenges. As discussed in Section 3.2, these challenges relate to scalability and performance limitations, interoperability and integration with existing systems, governance complexity arising from decentralized and multi-stakeholder control structures, and regulatory uncertainty combined with compliance challenges.

The reviewed studies indicate that these constraints frequently lead organizations to adopt cautious deployment strategies, rely on pilot projects, or implement hybrid and permissioned architectures to balance efficiency, control, and compliance (Treiblmaier, 2018; Xu et al., 2016).

Third, while Artificial Intelligence and Blockchain are often discussed within the same conceptual space, empirical evidence of deep interaction or strong complementarity between the two technologies remains limited.

When Artificial Intelligence and Blockchain are implemented jointly, organizational challenges do not simply accumulate but often interact, increasing governance complexity rather than reducing it.

As synthesized in Section 3.3, most studies describe parallel co-usage, in which AI and Blockchain operate in separate system layers and fulfill distinct functions.

A smaller body of research identifies functional complementarity at the technical level, particularly in contexts such as federated learning, explainable AI, and Blockchain-supported coordination mechanisms. However, these forms of integration are typically confined to experimental or domain-specific settings.

Only a limited subset of studies suggests organizational or governance-level interdependence, in which Blockchain-enabled transparency and auditability support oversight or accountability of AI systems. Even in these cases, the literature emphasizes that such complementarity is highly context-dependent and introduces additional governance complexity.

Overall, the findings indicate that organizational implementation challenges associated with Artificial Intelligence and Blockchain are largely technology-specific and predominantly addressed in isolation within the literature.

Although conceptual narratives frequently emphasize AI–Blockchain synergy, the empirical evidence reviewed in this thesis suggests that combined adoption is constrained by persistent organizational barriers at both the individual technology level and the level of integration.

4.2 Theoretical implications

The findings of this systematic literature review reinforce theoretical perspectives in the digital transformation literature that conceptualize Artificial Intelligence and Blockchain as socio-technical systems whose organizational impact is shaped primarily by governance structures, institutional legitimacy, and managerial capability rather than by technical feasibility alone (Verhoef et al., 2021; Vial, 2019).

With regard to Artificial Intelligence, the reviewed literature consistently links adoption barriers to issues of data governance, explainability, and institutional acceptance. Concerns related to transparency, trust, and accountability are not framed merely as limitations of algorithmic models, but as organizational challenges associated with oversight, responsibility allocation, and the justification of AI-driven decisions to internal and external stakeholders (Shrestha et al., 2019; Rahwan et al., 2019; Shneiderman, 2020).

These findings support governance-oriented theoretical perspectives on AI adoption, which emphasize that organizational legitimacy and managerial control are necessary complements to technical performance (Brynjolfsson & McAfee, 2017).

In the case of Blockchain, the findings align with theoretical views that conceptualize Blockchain as an organizational coordination infrastructure rather than solely as a technical system for secure record-keeping. Decentralized architectures redistribute decision rights, accountability boundaries, and control mechanisms across multiple actors, thereby introducing governance complexity as a structural implementation challenge (Treiblmaier, 2018; Xu et al., 2016; Tapscott & Tapscott, 2018).

This is particularly evident in consortium-based and cross-organizational settings, where ownership, authority, and compliance responsibilities are shared among participating organizations.

From a complementarity theory perspective, the findings refine prevailing theoretical claims by demonstrating that complementarity between Artificial Intelligence and Blockchain is not an inherent technological property, but a contingent organizational outcome shaped by governance and integration conditions.

Classical complementarity theory posits that value emerges when mutually reinforcing elements are jointly adopted as part of a coherent organizational configuration, implying that complementarities depend on alignment rather than mere co-adoption (Milgrom & Roberts, 1995; Brynjolfsson & Milgrom, 2013).

While conceptual narratives in the digital transformation literature often portray the combination of AI and Blockchain as inherently synergistic, the empirical literature reviewed in this study suggests that complementarity should not be treated as an inherent property of combining technologies (Tapscott & Tapscott, 2018).

Instead, complementarity emerges only when integration design choices, governance alignment, and institutional conditions are mutually reinforcing (Teece, 2018; Verhoef et al., 2021). In the absence of such alignment, the simultaneous adoption of Artificial Intelligence and Blockchain may increase governance complexity rather than generate complementary value.

In this sense, the findings highlight a theoretical gap between conceptual expectations of technological synergy and empirical patterns characterized by fragmented, cautious, and context-dependent integration.

Taken together, these findings suggest that complementarity theory must be applied with greater sensitivity to governance feasibility and institutional alignment when analyzing multi-technology digital transformation initiatives.

4.3 Practical implications

Building on the organizational implementation challenges identified in Chapter 3, the findings of this review translate into several practical implications for organizations considering the adoption of Artificial Intelligence, Blockchain, or combined initiatives.

1. Build governance before scaling:

The literature suggests that organizations benefit from treating governance as a prerequisite rather than an afterthought. For Artificial Intelligence, this entails formalizing data ownership, responsibility for data quality, and accountability for AI-driven outcomes. For Blockchain-based initiatives, this involves clearly defining decision rights, dispute resolution processes, and operational responsibilities across participating stakeholders.

2. Adopt problem-driven rather than technology-driven integration:

The reviewed studies indicate that combining Artificial Intelligence and Blockchain often increases architectural and governance complexity. Organizations are therefore advised to pursue integration only when a clearly defined organizational problem requires the joint use of both technologies, for example in cases where auditability, provenance, or multi-party coordination are essential to AI-related processes.

3. Choose architectures that match organizational maturity:

Given persistent challenges related to scalability and interoperability, organizations should select system architectures that they are capable of operating and governing over time. The literature suggests that permissioned or consortium-based Blockchain models may be more feasible in business contexts that prioritize compliance and control, even if this reduces the degree of decentralization.

4. Anticipate regulatory exposure early:

Regulatory uncertainty affects both technologies but is particularly constraining for Blockchain-based initiatives. The findings indicate that organizations benefit from involving legal and compliance expertise at an early stage, especially in cross-border or multi-stakeholder settings, and from avoiding assumptions that smart-contract automation reduces governance or compliance requirements.

Overall, the practical implication emerging from this review is that implementation success depends less on technological novelty and more on governance capability, integration readiness, and institutional alignment.

4.4 Limitations and directions for future research

This study is subject to several limitations. First, the review is based exclusively on published academic literature, which remains dominated by conceptual frameworks, exploratory analyses, and pilot implementations.

As a result, empirical evidence concerning long-term organizational outcomes and mature, enterprise-level deployments of combined Artificial Intelligence and Blockchain systems is limited.

Second, the findings reflect the scope of academic research rather than the full range of organizational practice. Many industry-led implementations and proprietary solutions are not systematically documented in peer-reviewed outlets and therefore fall outside the dataset.

Future research could address these limitations by conducting longitudinal case studies of organizations that have implemented Artificial Intelligence and Blockchain over extended periods. Comparative research across industries and regulatory regimes would further strengthen understanding of how organizational conditions shape interaction and complementarity between these technologies, particularly in multi-stakeholder environments.

4.5 Conclusion

This thesis synthesized the organizational implementation challenges associated with Artificial Intelligence and Blockchain and examined how the academic literature conceptualizes interaction and complementarity between these technologies. The findings demonstrate that, while both technologies hold significant transformative potential, their organizational value is constrained less by technological capability than by governance feasibility, accountability structures, and institutional alignment.

Although conceptual narratives frequently portray Artificial Intelligence and Blockchain as inherently complementary, the empirical literature reviewed in this study indicates that strong organizational or governance-level complementarity remains limited and highly context-dependent. Most reported implementations reflect parallel co-usage or partial technical integration rather than deep interdependence at the organizational level.

From a complementarity theory perspective, these findings suggest that complementarity between Artificial Intelligence and Blockchain should not be understood as an inherent technological property, but as a contingent organizational outcome that emerges only under specific conditions of integration design, governance alignment, and institutional support.

In the absence of such conditions, the simultaneous adoption of both technologies may increase coordination and governance complexity rather than generate complementary value.

Consequently, the combined adoption of Artificial Intelligence and Blockchain should be approached primarily as an organizational and institutional challenge rather than a purely technical one. Complementarity, where it occurs, must be deliberately designed and governed, rather than assumed to arise automatically from technological convergence.

References

- Alghamdi, S., Alruwaili, M., & Alotaibi, Y. (2022). Blockchain-empowered federated learning ecosystem for securing consumer IoT features analysis. *Sensors*, 22(18), 6786. <https://doi.org/10.3390/s22186786>
- Alibašić, H. (2025). A multi-paradigm ethical framework for hybrid intelligence in blockchain technology and cryptocurrency systems governance. *FinTech*, 4(3), Article 34. <https://doi.org/10.3390/fintech4030034>
- Biswas, K., Muthukkumarasamy, V., & Tan, W. L. (2024). Blockchain-enabled trustworthy federated learning systems. *IEEE Access*, 12, 21450–21465. <https://doi.org/10.1049/cmu2.12870>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Brynjolfsson, E., & Milgrom, P. (2012). Complementarity in organizations. In R. Gibbons & J. Roberts (Eds.), *The handbook of organizational economics* (pp. 11–55). Princeton University Press.
- Brynjolfsson, E., & McAfee, A. (2017). *Machine, platform, crowd: Harnessing our digital future*. W. W. Norton & Company.
- Djolev, D., Lazarova, M., & Nakov, O. (2024). FBLearn: Decentralized platform for federated learning on blockchain. *Electronics*, 13(19), 3672. <https://doi.org/10.3390/electronics13193672>
- Escorcia-Gutiérrez, J., Mansour, R., Leal, E., Villanueva, J., Jiménez-Cabas, J., Soto Montaña, C., & Soto Díaz, R. (2023). Privacy-preserving blockchain with energy-aware clustering scheme for IoT healthcare systems. *Mobile Networks and Applications*, 29, 1–12. <https://doi.org/10.1007/s11036-023-02115-9>
- Fasano, F., Bartoli, C., Cappa, F., & Boccardelli, P. (2025). Exploring the impact of artificial intelligence on Web3 decentralized platform business model innovation. *Journal of Engineering and Technology Management*, 78, 101911. <https://doi.org/10.1016/j.jengtecman.2025.101911>
- Hemdan, E. E.-D., & Sayed, A. (2025). Smart and secure healthcare with digital twins: A deep dive into blockchain, federated learning, and future innovations. *Algorithms*, 18(7), 401. <https://doi.org/10.3390/a18070401>
- Khaskheli, M. B., Zhao, Y., & Zhuo, Z. (2025). Sustainable maritime governance of digital technologies for marine economic development and for managing challenges in shipping risk: Legal policy and marine environmental management. *Sustainability*, 17(21), 9526. <https://doi.org/10.3390/su17219526>
- Kumar, P., Kumar, R., Aloqaily, M., & Islam, A. (2023). Explainable AI and blockchain for the metaverse: A security and privacy perspective. *IEEE Consumer Electronics Magazine*, 12, 1–7. <https://doi.org/10.1109/MCE.2023.3296222>
- Liang, Y., Li, Y., Shin, B.-S., & Shin, B.-S. (2024). Blockchain-based crowdsourcing for human intelligence tasks with dual fairness. *Blockchain: Research and Applications*, 5(4), 100213. <https://doi.org/10.1016/j.bcra.2024.100213>

- Lukić, I., Köhler, M., Krpić, Z., & Švaremajer, M. (2025). Advancing smart city sustainability through artificial intelligence, digital twin, and blockchain solutions. *Technologies*, 13(7), 300. <https://doi.org/10.3390/technologies13070300>
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications.
- Milgrom, P., & Roberts, J. (1990). The economics of modern manufacturing: Technology, strategy, and organization. *American Economic Review*, 80(3), 511–528.
- Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). Digital innovation management: Reinventing innovation management research in a digital world. *MIS Quarterly*, 41(1), 223–238. <https://doi.org/10.25300/MISQ/2017/41:1.03>
- Oktian, Y. E., Stanley, B., & Lee, S.-G. (2022). Building trusted federated learning on blockchain. *Symmetry*, 14(7), 1407. <https://doi.org/10.3390/sym14071407>
- Otoum, S., & Mouftah, H. T. (2021). Enabling trustworthiness in sustainable energy infrastructure through blockchain and AI-assisted solutions. *IEEE Wireless Communications*, 28(6), 19–25. <https://doi.org/10.1109/MWC.018.2100194>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. **BMJ**, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Peyvandi, A., Majidi, B., Peyvandi, S., et al. (2022). Privacy-preserving federated learning for scalable and high data quality computational-intelligence-as-a-service in Society 5.0. *Multimedia Tools and Applications*, 81, 25029–25050. <https://doi.org/10.1007/s11042-022-12900-5>
- Rahwan, I., Cebrian, M., Obradovich, N., et al. (2019). Machine behaviour. *Nature*, 568, 477–486. <https://doi.org/10.1038/s41586-019-1138-y>
- Rajawat, A. S., Goyal, S. B., Kumar, M., & Singh, T. P. (2023). An AI-enabled blockchain algorithm: A novel approach to counteract blockchain network security attacks. *EAI Endorsed Transactions on Internet of Things*. <https://doi.org/10.4108/eetiot.5484>
- Rajmohan, R., Kumar, T. A., Sandhya, S. G., et al. (2024). R-GCN: A residual-gated recurrent unit convolution network model for anomaly detection in blockchain transactions. *Multimedia Tools and Applications*, 83, 87527–87551. <https://doi.org/10.1007/s11042-023-17942-x>
- Rathod, T., Jadav, N. K., Tanwar, S., Polkowski, Z., Yamsani, N., Sharma, R., Alqahtani, F., & Gafar, A. (2023). AI and blockchain-based secure data dissemination architecture for IoT-enabled critical infrastructure. *Sensors*, 23(21), 8928. <https://doi.org/10.3390/s23218928>
- Rehman, A., Tariq, N., Ahmad Jan, M., Khan, F., Song, H., & Ibrahim, M. (2024). A blockchain-based hybrid model for IoMT-enabled intelligent healthcare system. *IEEE Transactions on Network Science and Engineering*, Advance online publication. <https://doi.org/10.1109/TNSE.2024.3376069>

- Salim, S., Turnbull, B., & Moustafa, N. (2021). A blockchain-enabled explainable federated learning for securing Internet-of-Things-based Social Media 3.0 networks. *IEEE Transactions on Computational Social Systems*, 8, 1–17. <https://doi.org/10.1109/TCSS.2021.3134463>
- Shahbazi, Z., & Byun, Y.-C. (2022). Blockchain-based event detection and trust verification using natural language processing and machine learning. *IEEE Access*, 10, 5790–5800. <https://doi.org/10.1109/ACCESS.2021.3139586>
- Shneiderman, B. (2020). Bridging the gap between ethics and practice: Guidelines for reliable, safe, and trustworthy human-centered AI systems. *ACM Transactions on Interactive Intelligent Systems*, 10(4), Article 26. <https://doi.org/10.1145/3419764>
- Shrestha, Y. R., Ben-Menahem, S. M., & von Krogh, G. (2019). Organizational decision-making structures in the age of artificial intelligence. *California Management Review*, 61(4), 66–83. <https://doi.org/10.1177/0008125619862257>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Sunmola, F., Baryannis, G., Tan, A., Co, K., & Papadakis, E. (2025). Holistic framework for blockchain-based halal compliance in supply chains enabled by artificial intelligence. *Systems*, 13(1), 21. <https://doi.org/10.3390/systems13010021>
- Tapscott, D., & Tapscott, A. (2018). *Blockchain revolution: How the technology behind bitcoin and other cryptocurrencies is changing the world* (Updated ed.). Penguin. <https://dontapscott.com/books/blockchain-revolution/>
- Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning*, 51(1), 40–49. <https://doi.org/10.1016/j.lrp.2017.06.007>
- Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Management: An International Journal*, 23(6), 545–559. <https://doi.org/10.1108/SCM-01-2018-0029>
- Truong, V. T., Le, H. D., & Le, L. B. (2024). Trust-free blockchain framework for AI-generated content trading and management in the metaverse. *IEEE Access*, 12, 41815–41828. <https://doi.org/10.1109/ACCESS.2024>
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection. *Journal of Business Research*, 122, 889–901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- Wahrstätter, A., Khan, S., & Svetinovic, D. (2024). OpenFL: A scalable and secure decentralized federated learning system on the Ethereum blockchain. *Internet of Things*, 26, 101174. <https://doi.org/10.1016/j.iot.2024.101174>
- Wang, Z., Li, Y., Li, D., Li, M., Zhang, B., Huang, S., & He, W. (2021). Enabling fairness-aware and privacy-preserving quality evaluation in vehicular crowdsensing: A decentralized approach. *Security and Communication Networks*, 2021, Article 9678409. <https://doi.org/10.1155/2021/9678409>

- Wang, K., Dong, J., Wang, Y., & Yin, H. (2019). Securing data with blockchain and AI. *IEEE Access*, 7, 77981–77989. <https://doi.org/10.1109/ACCESS.2019.2921555>
- Wang, J., et al. (2024). LearningChain: A highly scalable and applicable learning-based blockchain performance optimization framework. *IEEE Transactions on Network and Service Management*, 21(2), 1817–1831. <https://doi.org/10.1109/TNSM.2023.3347789>
- Wirata, G., Nugroho, Y., & Hidayanto, A. N. (2025). Organizational governance in AI–Blockchain ecosystems. *Information & Management*. Advance online publication. <https://doi.org/10.1016/j.im.2024.103808>
- Wu, Z., Liu, X., & Zhang, R. (2025). AI-driven blockchain supply chains: Network governance and corporate business model innovation in the Web3 era. *Journal of Technology Transfer*. <https://doi.org/10.1007/s10961-025-10300-z>
- Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The blockchain as a software connector. In *Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)* (pp. 182–191). IEEE. <https://doi.org/10.1109/WICSA.2016.21>
- Yang, S., Zheng, Y., & Chen, X. (2024). Regulatory governance of AI and Blockchain in multi-jurisdictional contexts. *Policy & Internet*, 16(1), 45–63. <https://doi.org/10.1002/poi3.348>
- Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). The new organizing logic of digital innovation: An agenda for information systems research. *Information Systems Research*, 21(4), 724–735. <https://doi.org/10.1287/isre.1100.0322>
- Zerka, F., et al. (2020). Artificial intelligence in healthcare: Ethical, legal and organizational challenges. *European Radiology*, 30(12), 6736–6746. <https://doi.org/10.1007/s00330-020-07043-2>

Appendix A – Article Memos

This appendix provides concise analytical memos for each of the studies included in the final synthesis. The memos summarize the focus of each study, the organizational implementation challenges addressed, and, where applicable, the type of interaction or complementarity between Artificial Intelligence and Blockchain. These memos form the empirical basis for the qualitative coding presented in Appendix B and support the synthesis in Chapter 3.

Zerka et al. (2020)

Context / focus:

AI applications in healthcare, with emphasis on data quality, bias, and ethical risks in distributed medical data environments.

Relevant organizational challenges:

AI: Data quality and dependency; ethical concerns, algorithmic bias, and accountability.

Interaction or complementarity:

Governance tension.

Relevance for this thesis:

Supports Sections 3.1.1 and 3.1.3 by demonstrating how data quality and ethical risks become organizational governance issues in AI-enabled healthcare systems.

Djolev et al. (2024)

Context / focus:

Blockchain-supported federated learning and AI coordination mechanisms.

Relevant organizational challenges:

AI: Data quality and dependency; explainability, transparency, and trust.

Blockchain: Scalability and performance limitations.

Interaction or complementarity:

Parallel co-usage.

Relevance for this thesis:

Informs Sections 3.1.1, 3.1.2, 3.2.1, and 3.3.1 by illustrating technical co-usage without deep organizational integration.

Alghamdi et al. (2022)

Context / focus:

AI adoption challenges in distributed data environments with regulatory considerations.

Relevant organizational challenges:

AI: Data quality and dependency; governance, regulation, and compliance.

Interaction or complementarity:

None identified.

Relevance for this thesis:

Contributes to Sections 3.1.1 and 3.1.4 by highlighting governance and compliance issues surrounding AI data management.

Otoum et al. (2021)

Context / focus:

AI systems in IoT and distributed analytics environments.

Relevant organizational challenges:

AI: Data quality and dependency.

Interaction or complementarity:

None identified.

Relevance for this thesis:

Supports Section 3.1.1 by showing how fragmented data sources constrain AI performance.

Peyvandi et al. (2022)

Context / focus:

Federated learning architectures and governance of shared data environments.

Relevant organizational challenges:

AI: Data quality and dependency; governance, regulation, and compliance.

Interaction or complementarity:

None identified.

Relevance for this thesis:

Relevant to Sections 3.1.1 and 3.1.4, emphasizing governance uncertainty in collaborative AI systems.

Escorcia-Gutierrez et al. (2024)

Context / focus:

Blockchain-based data sharing and AI coordination in complex digital ecosystems.

Relevant organizational challenges:

AI: Governance, regulation, and compliance.

Blockchain: Interoperability and system integration challenges.

Interaction or complementarity:

Functional complementarity.

Relevance for this thesis:

Supports Sections 3.2.2 and 3.3.2 by illustrating technical complementarity combined with integration challenges.

Witowski et al. (2021)

Context / focus:

Governance and regulatory considerations in AI-enabled decision-making systems.

Relevant organizational challenges:

AI: Governance, regulation, and compliance.

Interaction or complementarity:

None identified.

Relevance for this thesis:

Contributes to Section 3.1.4 by highlighting institutional and regulatory pressures on AI deployment.

Xu et al. (2016)

Context / focus:

Blockchain as a coordination layer for distributed systems and data exchange.

Relevant organizational challenges:

AI: Data quality and dependency.

Blockchain: Governance complexity.

Interaction or complementarity:

Functional complementarity.

Relevance for this thesis:

Supports Sections 3.2.3 and 3.3.2 by illustrating coordination-based complementarity.

Liang et al. (2024)

Context / focus:

Blockchain-enabled data validation mechanisms for AI training.

Relevant organizational challenges:

AI: Data quality and dependency.

Blockchain: Governance complexity.

Interaction or complementarity:

Functional complementarity.

Relevance for this thesis:

Relevant to Sections 3.1.1, 3.2.3, and 3.3.2.

Wang et al. (2019)

Context / focus:

Securing data through the combined use of Blockchain and Artificial Intelligence, with an emphasis on data integrity, access control, and intelligent threat detection.

Relevant organizational challenges:

AI: Dependence on high-quality data, transparency of AI-driven security mechanisms, and trust in automated decision-making.

Blockchain: Scalability constraints, computational overhead, and integration complexity with existing data infrastructures.

Interaction or complementarity:

Technical complementarity. AI is used to enhance data security analytics, while Blockchain provides immutable data storage and auditability.

Relevance for this thesis:

Informs Sections 3.1.1 and 3.3.3 by illustrating early forms of AI–Blockchain complementarity focused on technical security functions rather than organizational or governance-level integration.

Wang et al. (2021)

Context / focus:

AI bias and accountability in Blockchain-supported systems.

Relevant organizational challenges:

AI: Ethical concerns, algorithmic bias, and accountability.

Blockchain: Scalability and performance limitations.

Interaction or complementarity:

Governance tension.

Relevance for this thesis:

Informs Sections 3.1.3, 3.2.1, and 3.3.3 by showing how governance tensions arise in hybrid systems.

Wang et al. (2024)

Context / focus:

Optimization of blockchain system performance through machine learning, focusing on throughput and latency tuning using learning-based prediction models.

Relevant organizational challenges:

AI: Model reliability, data availability for training, and operational complexity of deploying learning-based optimization mechanisms.

Blockchain: Performance bottlenecks, scalability limitations, and the need for continuous parameter tuning in operational environments.

Interaction or complementarity:

Operational complementarity. AI models support adaptive performance optimization of Blockchain systems without altering core consensus mechanisms.

Relevance for this thesis:

Informs Sections 3.1.2 and 3.2.2 by demonstrating how AI complements Blockchain at an operational level, while also highlighting that such interaction primarily addresses technical efficiency rather than governance or accountability challenges.

Biswas et al. (2024)

Context / focus:

Explainable AI supported by Blockchain auditability mechanisms.

Relevant organizational challenges:

AI: Explainability, transparency, and trust.

Blockchain: Governance complexity.

Interaction or complementarity:

Functional complementarity.

Relevance for this thesis:

Directly supports Sections 3.1.2 and 3.3.2.

Oktian et al. (2022)

Context / focus:

Explainability challenges in AI-based systems.

Relevant organizational challenges:

AI: Explainability, transparency, and trust.

Interaction or complementarity:

None identified.

Relevance for this thesis:

Supports Section 3.1.2.

Wahrstätter et al. (2024)

Context / focus:

AI applications with Blockchain-based logging and verification.

Relevant organizational challenges:

AI: Explainability, transparency, and trust.

Blockchain: Scalability and performance limitations.

Interaction or complementarity:

Parallel co-usage.

Relevance for this thesis:

Supports Sections 3.1.2, 3.2.1, and 3.3.1.

Truong et al. (2024)

Context / focus:

Governance and accountability in AI–Blockchain ecosystems.

Relevant organizational challenges:

AI: Governance, regulation, and compliance.

Blockchain: Regulatory uncertainty and compliance challenges.

Interaction or complementarity:

Organizational interdependence.

Relevance for this thesis:

Supports Sections 3.1.4, 3.2.4, and 3.3.3

Yang et al. (2024)

Context / focus:

Regulatory governance of AI and Blockchain in multi-jurisdictional contexts.

Relevant organizational challenges:

AI: Governance, regulation, and compliance.

Blockchain: Regulatory uncertainty and compliance challenges.

Interaction or complementarity:

Organizational interdependence.

Relevance for this thesis:

Relevant to Sections 3.1.4, 3.2.4, and 3.3.3.

Kumar et al. (2024)

Context / focus:

Blockchain-based auditability for explainable and ethical AI.

Relevant organizational challenges:

AI: Explainability; ethical concerns, algorithmic bias, and accountability.

Blockchain: Governance complexity.

Interaction or complementarity:

Functional complementarity.

Relevance for this thesis:

Supports Sections 3.1.2, 3.1.3, and 3.3.2.

Salim et al. (2024)

Context / focus:

Hybrid AI–Blockchain architectures for trustworthy systems.

Relevant organizational challenges:

AI: Explainability, transparency, and trust.

Blockchain: Governance complexity.

Interaction or complementarity:

Functional complementarity.

Relevance for this thesis:

Supports Sections 3.1.2 and 3.3.2.

Rathod et al. (2023)

Context / focus:

Blockchain-supported explainable AI frameworks.

Relevant organizational challenges:

AI: Explainability, transparency, and trust.

Blockchain: Governance complexity.

Interaction or complementarity:

Functional complementarity.

Relevance for this thesis:

Supports Sections 3.1.2 and 3.3.2.

Alibašić (2025)

Context / focus:

Ethical governance and accountability in AI–Blockchain systems.

Relevant organizational challenges:

AI: Ethical concerns, algorithmic bias, and accountability; governance, regulation, and compliance. Blockchain:

Governance complexity.

Interaction or complementarity:

Organizational interdependence.

Relevance for this thesis:

Key source for Sections 3.1.3, 3.1.4, and 3.3.3.

Sunmola et al. (2025)

Context / focus:

Regulatory compliance in AI and Blockchain governance.

Relevant organizational challenges:

AI: Governance, regulation, and compliance.

Blockchain: Regulatory uncertainty and compliance challenges.

Interaction or complementarity:

Organizational interdependence.

Relevance for this thesis:

Supports Sections 3.1.4, 3.2.4, and 3.3.3.

Wirata et al. (2025)

Context / focus:

Governance design in AI–Blockchain ecosystems.

Relevant organizational challenges:

AI: Governance, regulation, and compliance.

Blockchain: Governance complexity.

Interaction or complementarity:

Organizational interdependence.

Relevance for this thesis:

Supports Sections 3.2.3 and 3.3.3.

Khaskheli et al. (2025)

Context / focus:

Regulatory and institutional challenges in decentralized digital systems.

Relevant organizational challenges:

AI: Governance, regulation, and compliance.

Blockchain: Regulatory uncertainty and compliance challenges.

Interaction or complementarity:

Organizational interdependence.

Relevance for this thesis:

Relevant to Sections 3.1.4, 3.2.4, and 3.3.3.

Wu et al. (2025)

Context / focus:

Decentralized governance mechanisms in Blockchain-enabled systems.

Relevant organizational challenges:

AI: Governance, regulation, and compliance.

Blockchain: Governance complexity.

Interaction or complementarity:

Organizational interdependence.

Relevance for this thesis:

Supports Sections 3.2.3 and 3.3.3.

Lukić et al. (2025)

Context / focus:

Blockchain governance and regulatory coordination in cross-sector ecosystems.

Relevant organizational challenges:

AI: Governance, regulation, and compliance.

Blockchain: Regulatory uncertainty and compliance challenges.

Interaction or complementarity:

Organizational interdependence.

Relevance for this thesis:

Supports Sections 3.2.4 and 3.3.3.

Fasano et al. (2025)

Context / focus:

Governance tensions in decentralized digital infrastructures.

Relevant organizational challenges:

AI: Governance, regulation, and compliance.

Blockchain: Governance complexity.

Interaction or complementarity:

Organizational interdependence.

Relevance for this thesis:

Supports Sections 3.2.3 and 3.3.3.

Tekchandani et al. (2025)

Context / focus:

Blockchain scalability optimization.

Relevant organizational challenges:

Blockchain: Scalability and performance limitations.

Interaction or complementarity:

Parallel co-usage.

Relevance for this thesis:

Supports Section 3.2.1.

Rajmohan et al. (2024)

Context / focus:

Performance optimization in Blockchain environments.

Relevant organizational challenges:

Blockchain: Scalability and performance limitations.

Interaction or complementarity:

Parallel co-usage.

Relevance for this thesis:

Supports Section 3.2.1.

Hemdan and Mahmoud (2025)

Context / focus:

Blockchain interoperability in IoT and smart systems.

Relevant organizational challenges:

Blockchain: Interoperability and system integration challenges.

Interaction or complementarity:

Weak complementarity.

Relevance for this thesis:

Supports Section 3.2.2.

Rehman et al. (2024)

Context / focus:

Legacy system integration with Blockchain architectures.

Relevant organizational challenges:

Blockchain: Interoperability and system integration challenges.

Interaction or complementarity:

Weak complementarity.

Relevance for this thesis:

Supports Section 3.2.2.

Appendix B: Coding Overview Table

This appendix provides a transparent overview of how the studies included in the final synthesis were coded across the analytical dimensions applied in this systematic literature review. The table summarizes how each study contributes to the analysis of **(1)** AI-related organizational challenges, **(2)** Blockchain-related organizational challenges, and **(3)** the type and nature of interaction or complementarity between Artificial Intelligence and Blockchain.

Each study was coded across three analytical dimensions:

1. AI-related organizational challenges,
2. Blockchain-related organizational challenges,
3. Type of interaction or complementarity between Artificial Intelligence and Blockchain.

A dash (—) indicates that the study did not substantively address organizational challenges related to the respective technology. Interaction or complementarity types were coded only when the study explicitly discussed functional, organizational, or governance-related relationships between Artificial Intelligence and Blockchain, in line with the analytical framework applied in Section 3.3.

Study	AI-related organizational challenges	Blockchain-related organizational challenges	Interaction / complementarity type
Zerka et al. (2020)	Data quality and data dependency; ethical concerns, algorithmic bias, and accountability	—	Governance tension
Djolev et al. (2024)	Data quality and data dependency; explainability, transparency, and trust	Scalability and performance limitations	Parallel co-usage
Alghamdi et al. (2022)	Data quality and data dependency; governance, regulation, and compliance	—	—
Otoum et al. (2021)	Data quality and data dependency	—	—
Peyvandi et al. (2022)	Data quality and data dependency; governance, regulation, and compliance	—	—

Study	AI-related organizational challenges	Blockchain-related organizational challenges	Interaction / complementarity type
Escorcia-Gutierrez et al. (2024)	Governance, regulation, and compliance	Interoperability and system integration challenges	Functional complementarity
Witowski et al. (2021)	Governance, regulation, and compliance	—	—
Xu et al. (2016)	Data quality and data dependency	Governance complexity	Functional complementarity
Liang et al. (2024)	Data quality and data dependency	Governance complexity	Functional complementarity
Wang et al. (2021)	Ethical concerns, algorithmic bias, and accountability	Scalability and performance limitations	Governance tension
Biswas et al. (2024)	Explainability, transparency, and trust	Governance complexity	Functional complementarity
Oktian et al. (2022)	Explainability, transparency, and trust	—	—
Wahrstätter et al. (2024)	Explainability, transparency, and trust	Scalability and performance limitations	Parallel co-usage
Truong et al. (2024)	Governance, regulation, and compliance	Regulatory uncertainty and compliance challenges	Organizational interdependence
Yang et al. (2024)	Governance, regulation, and compliance	Regulatory uncertainty and compliance challenges	Organizational interdependence
Kumar et al. (2024)	Explainability, transparency, and trust; ethical concerns, algorithmic bias, and accountability	Governance complexity	Functional complementarity
Salim et al. (2024)	Explainability, transparency, and trust	Governance complexity	Functional complementarity
Rathod et al. (2023)	Explainability, transparency, and trust	Governance complexity	Functional complementarity
Alibašić (2025)	Ethical concerns, algorithmic bias, and accountability; governance, regulation, and compliance	Governance complexity	Organizational interdependence

Study	AI-related organizational challenges	Blockchain-related organizational challenges	Interaction / complementarity type
Sunmola et al. (2025)	Governance, regulation, and compliance	Regulatory uncertainty and compliance challenges	Organizational interdependence
Wirata et al. (2025)	Governance, regulation, and compliance	Governance complexity	Organizational interdependence
Khaskheli et al. (2025)	Governance, regulation, and compliance	Regulatory uncertainty and compliance challenges	Organizational interdependence
Wu et al. (2025)	Governance, regulation, and compliance	Governance complexity	Organizational interdependence
Lukić et al. (2025)	Governance, regulation, and compliance	Regulatory uncertainty and compliance challenges	Organizational interdependence
Fasano et al. (2025)	Governance, regulation, and compliance	Governance complexity	Organizational interdependence
Tekchandani et al. (2025)	—	Scalability and performance limitations	Parallel co-usage
Rajmohan et al. (2024)	—	Scalability and performance limitations	Parallel co-usage
Hemdan & Mahmoud (2025)	—	Interoperability and system integration challenges	Weak complementarity
Rehman et al. (2024)	—	Interoperability and system integration challenges	Weak complementarity