

Governing digital finance in cyberspace: An integrated review of cyber resilience, trust, and responsible AI for sustainable economic development

Seyed Alireza Khezri*, Farzin Rezaei

Department of Accounting, Qa .c., Isalamic Azad university, Qazvin, Iran.

(*Corresponding author:  alireza.khezri9232@iau.ac.ir,  <https://orcid.org/0009-0008-4505-9627>)

Article Info	Abstract
Original article	Background: Digital finance is fundamentally restructuring global financial systems, yet governance frameworks remain fragmented and lag behind rapid technological change, exposing critical vulnerabilities in cyber resilience, digital trust, and responsible artificial intelligence. Aims: This study addresses this gap. Methodology: A systematic meta-synthesis of 30 peer-reviewed studies, including 24 studies published between 2025 and 2026 and six foundational theoretical or conceptual studies published between 2022 and 2024, integrating institutional theory and socio-technical systems theory to develop a holistic governance framework were conducted. Findings: The analysis reveals five interconnected dimensions: governance mechanisms, cyber resilience, digital trust, responsible AI, and sustainable economic development that are conceptually interdependent and mutually constitutive, suggesting a co-evolutionary dynamic that is advanced here as a theoretical proposition for future longitudinal investigation. Key findings expose persistent tensions between state-centric and multi-stakeholder governance models, a significant implementation gap between responsible AI principles and operational practices, and a paradoxical relationship wherein digital financial inclusion may inadvertently undermine environmental sustainability. Conclusion: The study advances theoretical understanding by extending institutional theory to cyberspace governance and highlighting the mutual implication of socio-technical elements in digital finance a co-evolutionary dynamic that we propose for future empirical testing. Practically, it provides actionable insights for policymakers, regulators, and financial institutions to align technological innovation with resilience, trust, and sustainability objectives. This integrated framework offers a robust foundation for future research on adaptive governance in increasingly complex digital financial systems, emphasising the necessity of cross-sectoral coordination and context-sensitive policy design.
Main Object: Computer Science & Technology	
Received: 25 July 2026	
Revised: 05 September 2026	
Accepted: 11 September 2026	
Published online: 23 September 2026	
Keywords: cyber resilience, digital finance governance, digital trust, responsible artificial intelligence, Socio technical systems, Sustainable Development Goals (SDGs).	

Cite this article: Khezri SA, Rezaei F. (???). "Governing digital finance in cyberspace: An integrated review of cyber resilience, trust, and responsible AI for sustainable economic development". *Cyberspace Studies*. ?(?): 1-36. doi: <https://doi.org/10.22059/jcss.2026.419307.1269>.



Creative Commons Attribution-NonCommercial 4.0 International License
Website: <https://jcss.ut.ac.ir/> Email: jcss@ut.ac.ir |
EISSN: 2588-5502
Publisher: University of Tehran

1. Introduction

Digital transformation is fundamentally reconfiguring the architecture of the global financial system. Traditional finance historically grounded in centralized intermediation, physical documentation, and relational trust is increasingly being replaced by a digitally mediated ecosystem characterized by platform-based interactions, algorithmic decision-making, and data-driven financial services (World Bank, 2022; Ferrari, 2022; Vărzaru & Bocean, 2024; Shan, 2026). Innovations such as digital banking, mobile payments, decentralized finance (DeFi), and central bank digital currencies (CBDCs) are not merely technological upgrades; they represent a structural shift in how financial value is created, governed, and exchanged (Dionysopoulos et al., 2024; Sanz Bayón, 2025; Gafsi, 2025). Consequently, the contemporary financial system is best understood not as a purely technical infrastructure, but as a socio-technical institutional system in which technologies, actors, and governance arrangements co-evolve (Bolton & Foxon, 2015; Volz et al., 2025; Vaya-Arboledas et al., 2025; Wafi et al., 2026; Santos, 2026).

Within this transformation, three interrelated challenges have emerged as central to the stability and legitimacy of digital finance (Dafri & Al-Qaruty, 2023; Hordofa, 2024; Jin & Xie, 2024; Al-Okaily & Al-Okaily, 2025). First, governance in cyberspace presents a fundamental institutional dilemma. Unlike traditional financial systems bounded by national jurisdictions, digital finance operates across decentralized and borderless networks, rendering conventional regulatory models increasingly inadequate (Goldstein & Narayanaswamy, 2025; Teng et al., 2026). This raises critical questions regarding the design of governance mechanisms capable of balancing innovation with financial stability and inclusion, while accommodating the transnational nature of digital financial activities. Second, the growing exposure of financial systems to cyber threats has elevated cyber resilience from a technical concern to a systemic imperative (Bagherifam et al., 2025; Webb & Sallos, 2025; Ghosh & Golder, 2026). Financial infrastructures are now deeply embedded in interconnected digital networks, making them vulnerable to sophisticated and evolving cyber risks. However, existing approaches to cyber resilience remain largely fragmented, often emphasizing technical defenses while overlooking institutional coordination and economic implications. Third, the transformation of trust in digital environments constitutes a foundational challenge (Amofa et al., 2026; Mai et al., 2025; Vuković et al., 2025; Tzavara & Vassiliadis, 2024; Singh et al., 2025; Islam, 2026). As financial interactions become increasingly mediated by algorithms and data infrastructures, trust shifts from interpersonal and institutional familiarity to confidence in technological systems, data integrity, and algorithmic transparency. Yet, the conceptualization and operationalization of digital trust remain insufficiently developed, particularly in relation to governance and

technological design (Sathiskumar & Andersen, 2025; Dang & Li, 2026; Jang, 2026; Giannitsas et al., 2026; Salem, 2026; Galindez-Acosta & Giraldo-Huertas, 2026; Shao et al., 2026; Hidayat-ur-Rehman et al., 2026).

Artificial intelligence (AI) intensifies and simultaneously mediates these challenges. On the one hand, AI enhances efficiency, risk assessment, fraud detection, and financial inclusion through advanced analytics and automation (Marak & Ayyagari, 2025; Alahmad et al., 2026; Li, 2026; Siddik & Amin, 2026). On the other hand, it introduces critical concerns related to algorithmic bias, opacity, accountability, and data governance (Kango, 2025; Nouis et al., 2025; Lendvai & Gosztanyi, 2025; Wang et al., 2026). As Shahghasemi (2026) argues, the concentration of epistemic power in AI systems raises fundamental questions about democratic oversight and the governance of knowledge production in digital ecosystems. These tensions have led to the emergence of Responsible AI as a necessary paradigm for aligning technological capabilities with ethical, legal, and societal expectations. Despite growing scholarly attention, existing research on AI in finance remains fragmented, with limited integration between ethical principles, governance structures, trust formation, and system resilience (Ricciardi Celsi & Zomaya, 2025; Kasarci et al., 2025; Papagiannidis et al., 2025; Parthasarathy & Panigrahi, 2026).

At a broader level, these challenges converge in the context of sustainable economic development. Digital finance is increasingly recognized as a key enabler of the Sustainable Development Goals (SDGs), particularly through mechanisms such as financial inclusion, transparency, risk mitigation, and data-driven decision-making (Tay et al., 2022; Danladi et al., 2023; Raihan, 2024; Värzaru, 2025; Kumari et al., 2025; Meniago, 2025). Extending this perspective, (Khezri & Rezaei, 2026) systematically mapped the convergence of blockchain, IoT, and artificial intelligence, demonstrating that their synergistic integration while currently empirically scarce offers critical pathways for responsible investment and SDG advancement through enhanced transparency, real-time sensing, and predictive intelligence. However, the effectiveness of these mechanisms depends on the presence of coherent governance frameworks, resilient infrastructures, trustworthy systems, and ethically aligned AI. The absence of integration among these dimensions limits both theoretical understanding and practical implementation of sustainable digital finance (Perboli et al., 2025; Aarab et al., 2025; Kim, 2026; Raihan & Sarker, 2026). The 17 Sustainable Development Goals of the United Nations are set forth in Figure 1.



Figure 1. United Nations general assembly, 2025

A critical review of the literature reveals a persistent fragmentation across four key domains: digital finance governance, cyber resilience, digital trust, and responsible AI. Existing studies have largely examined these domains in isolation, resulting in three major limitations (Lezzi et al., 2025). First, there is a lack of cross-domain integration that explains how governance structures, technological systems, and behavioral factors interact. Second, the underlying mechanisms through which these elements jointly influence financial stability and sustainability remain underexplored. Third, limited attention has been given to the co-evolutionary dynamics that characterize digital financial systems, particularly in the context of cyberspace. As a result, there is a clear need for an integrated analytical framework that captures the interdependencies among these dimensions.

To address this gap, this study draws upon Institutional Theory and Socio-Technical Systems Theory as complementary analytical lenses. Institutional Theory provides a foundation for understanding how rules, norms, and governance arrangements shape organizational behavior and system legitimacy in digital finance (Lawrence & Shadnam, 2008; Hwang, 2023; Bağcı et al., 2026; Amofa et al., 2026). However, in the context of cyberspace, traditional institutional assumptions such as territoriality and centralized authority require reconsideration. Socio-Technical Systems Theory complements this perspective by emphasizing the inseparability of technological and social elements, highlighting how system outcomes emerge from the dynamic interaction between infrastructures, actors, and institutional contexts (Savaş & Karataş, 2022; Mumford & Shires, 2023; Fratini, 2025; Lu et al., 2025; Shahghasemi, 2025). The integration of these theories enables a co-evolutionary perspective in which governance, resilience, trust, and AI are conceptualized as mutually constitutive rather than independent components. While our cross-sectional data cannot

empirically confirm temporal co-evolution, the synthesis reveals strong patterns of mutual implication that justify advancing co-evolution as a theoretical proposition one that awaits testing through longitudinal and historical research designs. Accordingly, the primary research question guiding this study is: What are the components of an integrated digital finance governance framework in cyberspace that simultaneously incorporates cyber resilience, digital trust, and responsible AI, and how do their interactions contribute to sustainable economic development?

To operationalize this inquiry, the study addresses the following sub-questions: (1) What constitutes effective governance in digital financial systems operating in cyberspace? (2) How can cyber resilience be defined and assessed in relation to financial stability? (3) What are the core dimensions of digital trust in AI-enabled financial systems, and how can they be strengthened? (4) What principles and mechanisms define responsible AI in digital finance, and how are they embedded within governance structures? (5) How do these components co-evolve to support sustainable economic outcomes?

The contribution of this study is threefold. Theoretically, it advances the literature by integrating previously fragmented domains into a coherent conceptual framework grounded in complementary theoretical perspectives. Methodologically, it employs a systematic integrated review combined with meta-synthesis to generate higher-order insights that extend beyond descriptive aggregation. Practically, it provides a structured framework to guide policymakers, regulators, and financial institutions in designing digital financial systems that are resilient, trustworthy, and aligned with sustainable development objectives.

2. Methodology

2.1. Research design and integrated review protocol

This study employed a qualitative exploratory design to investigate the governance of digital finance in cyberspace, with particular emphasis on the interconnected domains of cyber resilience, digital trust, and responsible artificial intelligence within the context of sustainable economic development. To construct a comprehensive and empirically grounded analytical framework, an integrated review combined with meta-synthesis was conducted, following the seven-phase methodological framework proposed by Sandelowski and Barroso (2007). This approach was selected for its demonstrated efficacy in synthesizing qualitative and mixed-methods research while preserving the richness and contextual nuances of primary studies. All identified records were exported to a reference management software (EndNote) for duplicate detection and removal. Duplicates were identified automatically based on title, author, and DOI matching, followed by a manual cross-verification to ensure accuracy and eliminate false positives. All records retrieved from the four databases were exported to EndNote for duplicate detection and removal. Duplicate records were

identified using automated matching based on titles, authors, and DOIs and were then manually checked to minimise erroneous exclusions. After this process, 739 unique records remained for title screening.

A systematic literature search was performed across four major electronic databases: Scopus, Web of Science, IEEE Xplore, ACM Digital Library. The search timeframe was deliberately constrained to the period from 2025 to 2026. This focused window was chosen for three interrelated reasons. First, the post-2024 period has witnessed an unprecedented acceleration in the deployment of generative AI and large language models in financial services, creating novel governance challenges not previously documented. Second, major regulatory frameworks such as the EU AI Act and various national AI strategies have begun implementation only from 2025 onward, making this period a critical juncture for examining emerging governance practices. Third, the 2025–2026 timeframe captures the most recent empirical evidence available at the time of the review, ensuring the synthesis reflects the current state of the field rather than outdated patterns. While we acknowledge that a two-year window cannot capture long-term evolutionary trends, this focused scope is justified as a 'state-of-the-art snapshot' rather than a historical analysis. To partially address this limitation and provide theoretical grounding, we also included six seminal theoretical and conceptual studies published between 2022 and 2024 that offer foundational definitions and frameworks not time-sensitive to the analysis. A Boolean search string was constructed and applied to titles, abstracts, and keywords, combining terms across four thematic clusters: (1) digital finance governance ("digital finance" OR "fintech" OR "digital banking" OR "central bank digital currency" OR "CBDC" OR "decentralized finance" OR "DeFi"), (2) cyber resilience ("cyber resilience" OR "cybersecurity" OR "cyber risk" OR "information security" OR "digital resilience"), (3) trust and AI ("digital trust" OR "algorithmic trust" OR "responsible AI" OR "ethical AI" OR "AI governance" OR "explainable AI"), and (4) sustainability ("sustainable development" OR "SDG" OR "financial stability" OR "economic sustainability" OR "inclusive finance").

2.2. Selection process and inclusion criteria

The study selection rigorously adhered to the PRISMA 2020 guidelines (Page et al., 2021), progressing through three sequential screening stages: (1) title review, (2) abstract screening, and (3) full-text eligibility assessment. The inclusion criteria were established as follows: (a) peer-reviewed empirical studies (qualitative, quantitative, or mixed-methods) or theoretical/conceptual articles demonstrating clear methodological transparency and theoretical rigor; (b) studies explicitly addressing governance mechanisms, resilience frameworks, trust dynamics, or AI ethics within digital financial systems, with substantive focus on institutional, regulatory, or socio-technical

dimensions; (c) publications in English, with no geographical restrictions to ensure comprehensive coverage of diverse regulatory and institutional contexts. Exclusion criteria encompassed non-systematic reviews, opinion pieces, editorials, book chapters, conference abstracts, technical reports without theoretical grounding, and articles lacking full-text accessibility. Additionally, studies focusing exclusively on technical aspects without addressing governance, trust, or sustainability dimensions were excluded.

2.2.1. Inclusion criteria

- Articles and research outputs published within the specified field of inquiry (digital finance governance, cyber resilience, digital trust, responsible AI, and sustainable economic development);
- Qualitative, quantitative, or mixed methods studies that yield findings relevant to the subject matter;
- Investigations reporting sufficient data and information germane to the research objectives;
- Research that has undergone a peer review process and has been disseminated as a complete, full length article;
- Articles and research published between 2025 and 2026, inclusive. Additionally, to ensure robust theoretical grounding, we included six seminal theoretical and conceptual studies published between 2022 and 2024 (specifically, Vărzaru & Bocean, 2024; Hordofa, 2024; Yusif et al., 2024; Tzavara & Vassiliadis, 2024; Hanisch et al., 2023; Savaş & Karataş, 2022). These works provide foundational definitions and conceptual frameworks that are not time-sensitive but are essential for establishing the theoretical backbone of this meta-synthesis. Their inclusion was justified by their high quality scores (>31 on CASP) and their specific relevance to defining core constructs.
- Studies that have scientifically examined the topic and have proposed appropriate, context sensitive solutions for implementing effective governance, resilience, trust, and responsible AI in digital financial systems.

2.3. Data extraction and thematic synthesis

A standardized data extraction protocol was developed to systematically capture pertinent information from each included study: author(s)/year, geographical and institutional context, theoretical underpinnings, methodological approach, digital finance domain examined, governance mechanisms and regulatory frameworks, cyber resilience strategies and tools, trust-building mechanisms and measurement approaches, AI applications and responsible AI principles, sustainability outcomes and SDG alignment, and key

challenges and limitations identified. The extracted data were subjected to a three-level thematic synthesis embedded within the meta-synthesis framework:

- **Open coding:** Identifying and labelling discrete concepts, factors, and relationships (e.g., "regulatory fragmentation in cross-border digital finance", "algorithmic opacity in credit scoring", "institutional trust deficits", "cyber resilience capability maturity", "data sovereignty tensions", "explainability requirements for AI-driven risk assessment");
- **Axial coding:** Grouping codes into broader conceptual categories through iterative comparison and relationship mapping (e.g., "institutional governance mechanisms", "cyber resilience dimensions", "digital trust antecedents and outcomes", "responsible AI principles and implementation frameworks", "sustainability enablers and barriers", "socio-technical interdependencies");
- **Selective coding:** Synthesizing categories into overarching explanatory themes, which formed the foundation of the proposed integrated governance framework addressing the convergence of digital finance governance, cyber resilience, digital trust, and responsible AI for sustainable economic development.

A notable limitation of this study is its restricted temporal scope (2025-2026). This two-year snapshot, while intentionally focused on capturing the most recent developments in AI-driven financial governance, cannot capture long-term evolutionary trends or confirm co-evolutionary dynamics over extended periods. Future longitudinal research is required to test the temporal propositions advanced in this synthesis.

To ensure coding reliability and analytical rigor, two independent researchers with expertise in digital finance governance, information systems, and institutional theory coded all selected articles separately. The unit of analysis was the individual coding segment, defined as a distinct statement, claim, or finding extracted from each study that was directly relevant to the research questions. A total of 426 coding segments were identified across the 30 articles. The coding framework consisted of five pre-defined thematic categories derived from the research questions (Governance, Cyber Resilience, Digital Trust, Responsible AI, and Sustainability), supplemented by emergent codes identified through open coding. Inter-coder agreement was assessed using Cohen's Kappa statistic via SPSS, yielding a coefficient of 0.921 ($P < 0.001$), indicating "almost perfect agreement" according to Landis and Koch (1977). Discrepancies were resolved through consensus discussion and, where necessary, adjudication by a third expert reviewer.

Nature of the corpus and management of overlapping evidence of the 30 studies included in this meta-synthesis. 18 are systematic literature reviews or meta-analyses, while 12 are empirical or conceptual primary studies. Consequently, this investigation constitutes a meta-synthesis of reviews supplemented by primary evidence an approach justified when the goal is to generate higher-order theoretical insights by synthesising interpretive claims across multiple review-level contributions. To mitigate the risk of double-counting the same primary evidence, we adopted three methodological precautions: (a) we did not extract data from primary studies that were already comprehensively covered in the included reviews; (b) where multiple reviews cited the same primary study, we counted that primary study only once and only extracted its findings if they were independently corroborated across at least two reviews; and (c) we treated the included reviews primarily as data sources representing the *interpretive conclusions* of their authors, rather than as raw repositories of primary evidence. This approach ensures that our synthesis reflects thematic convergence across reviews while minimising the risk of artefactual inflation.

2.4. Trustworthiness and reflexivity

To establish the trustworthiness of the meta-synthesis, the study employed Lincoln and Guba's (1985) four criteria: credibility, transferability, dependability, and confirmability. Credibility was enhanced through independent dual coding, external review by a third expert, and triangulation across multiple theoretical perspectives (Institutional Theory and Socio-Technical Systems Theory). Dependability and confirmability were ensured by maintaining a detailed reflexive journal documenting all methodological decisions, coding rules, interpretive choices, and theoretical refinements throughout the research process, as well as providing a transparent audit trail accessible for external scrutiny. Transferability was supported by providing thick descriptions of the search strategy, inclusion criteria, database coverage, and contextual characteristics of the selected studies (including geographical diversity across developed and emerging economies, institutional settings, regulatory regimes, and technological maturity levels). All methodological procedures, including the PRISMA flowchart, detailed search strings, quality assessment scores, and coding frameworks, are presented in the Results section to guarantee transparency, reproducibility, and methodological integrity.

3. Results

3.1. Qualitative findings

Within the overarching methodological framework of this meta-synthesis, secondary data and empirical evidence extracted from prior scholarly works were systematically integrated to generate novel theoretical insights and adequately address the predefined research

questions concerning the governance of digital finance in cyberspace, with particular emphasis on cyber resilience, digital trust, and responsible artificial intelligence. This integrative approach enabled the identification of core categorical constructs and evaluative criteria that significantly shape the successful deployment of governance frameworks, resilience mechanisms, trust-building strategies, and ethical AI principles within digital financial ecosystems. Consequently, it facilitated the optimisation of regulatory policies, risk management protocols, cybersecurity infrastructures, and transparency-accountability mechanisms in digitally mediated financial systems. The meta-synthesis was rigorously operationalised in accordance with the procedural guidelines proposed by Sandelowski and Barroso (2007), a methodological stance that concurrently permitted both a comprehensive interrogation of the extant literature and the methodical extraction of central thematic elements across institutional, regulatory, technological, and developmental domains. The Seven-Step Meta-Synthesis Model is set forth in Figure 2.

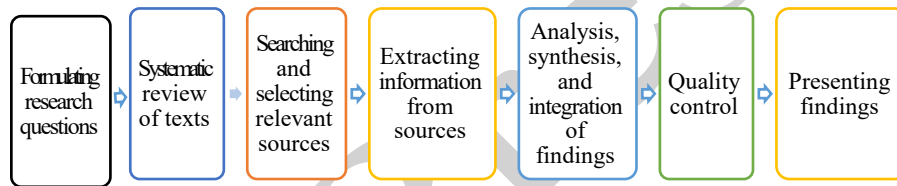


Figure 2. The seven-step meta-synthesis model (adapted from Sandelowski & Barroso, 2007)

3.2. Formulation of research questions

During the initial phase of the meta-synthesis process, the research questions were carefully formulated with the explicit objective of identifying the underlying factors that shape digital finance governance, cyber resilience dimensions, digital trust components, and responsible AI principles, as well as their consequent institutional, regulatory, technological, and developmental implications for policymakers, financial institutions, and industry stakeholders. The Research Questions are presented in Table 1.

4. Systematic literature review

For the purposes of the present investigation, a systematic retrieval of relevant English language sources was undertaken from reputable scientific repositories, namely Scopus, Web of Science, IEEE Xplore, ACM Digital Library, employing targeted keyword search strategies. The selection process was deliberately oriented toward identifying the most germane body of literature pertaining to digital finance governance, cyber resilience frameworks, trust dynamics in financial systems, responsible and ethical AI principles, and the interlinkages

between these dimensions and sustainable economic development, thereby ensuring a comprehensive and methodologically sound overview of contemporary research within these intersecting domains.

Table 1. Research questions

Research question / Parameter	Specification
Identifying the criteria that influence digital finance governance, cyber resilience, digital trust, and responsible AI in the context of sustainable economic development.	What
Peer-reviewed scholarly sources addressing digital finance governance, cyber resilience, digital trust, responsible AI, and sustainable economic development.	Who
Encompassing all works from 2025 to 2026 ¹ .	When
Thematic review, identification and note-taking, key insights extraction, conceptual analysis, and synthesis of governance, technical, and developmental strategies.	How

4.1. Search and selection of relevant texts

Following the initial resource retrieval, it became imperative to screen the identified studies against predefined criteria in order to select only relevant, high-quality research for subsequent analysis. These criteria served to delineate the inclusion and exclusion boundaries of studies, with the overarching aim of selecting the most pertinent and methodologically robust research contributions aligned with the research topic. The inclusion and exclusion criteria are articulated as follows.

Inclusion criteria

- Articles and research outputs published within the specified field of inquiry (digital finance governance, cyber resilience, digital trust, responsible AI, and sustainable economic development);
- Qualitative, quantitative, or mixed-methods studies that yield findings relevant to the subject matter (governance, regulatory, technological, trust-related, or developmental dimensions);
- Investigations reporting sufficient data and information germane to the research objectives (governance frameworks, resilience strategies, trust-building mechanisms, ethical AI principles, sustainability indicators);
- Research that has undergone a peer-review process and has been disseminated as a complete, full-length article.
- Articles and research published between 2025 and 2026, inclusive;
- Studies that have scientifically examined the topic and have proposed appropriate, context-sensitive solutions for

1. The primary database search covered studies published between 2025 and 2026. Six earlier peer-reviewed studies published between 2022 and 2024 were purposively retained as foundational theoretical or conceptual sources and are reported separately from the primary search corpus.

implementing effective governance, resilience, trust, and responsible AI in digital financial systems.

Exclusion criteria

- Research that fails to report sufficient information relevant to the research objectives;
- Studies conducted with identical titles and overlapping objectives (duplicate or redundant works);
- Research lacking an appropriate methodological framework or scientific rigour;
- Research published in journals of low scholarly standing or non-peer-reviewed outlets;
- Conference abstracts, editorials, opinion pieces, and book chapters.

4.2. Quality assessment protocol

For the qualitative appraisal of article quality, we developed a custom quality assessment instrument informed by the Critical Appraisal Skills Programme (CASP) framework. While the original CASP employs yes/no/can't-tell responses, we adapted it to a semi-quantitative 5-point Likert scale (1= very poor to 5= excellent) across ten criteria to allow for fine-grained differentiation among the included studies, yielding a maximum possible score of 50. This adapted instrument is explicitly labelled as a CASP-informed custom tool rather than the original CASP checklist. The cutoff threshold of 31 (out of 50) was chosen conservatively to ensure that only studies with 'Very Good' (31–40) or 'Excellent' (41–50) methodological quality were included in the synthesis. Although studies scoring 21–30 ('Good') may have valuable insights, the meta-synthesis approach requires a higher evidentiary baseline to minimize bias and ensure theoretical robustness; hence, the 'Good' category was intentionally excluded to maintain analytical rigor.

This categorical stratification facilitated the selection of the most appropriate, credible, and methodologically sound sources for the final analytical phase. Table 2 subsequently presents the outcomes of the article evaluations based on the CASP methodology, alongside the key criteria employed for the adjudication and inclusion of approved articles. The Specifications of the CASP Assessment Questions are set forth in Table 2.

The screening and selection process followed the PRISMA 2020 reporting framework. After duplicate removal and manual verification, 739 unique records remained for title screening. At the title-screening stage, 135 records were excluded because they were thematically irrelevant, leaving 604 records for abstract screening. A further 259 records were excluded at the abstract-screening stage because they did not address the core domains of digital finance governance, cyber resilience, digital trust, responsible AI, or sustainable development. The

remaining 345 records underwent full-text eligibility assessment. Of these, 297 were excluded because they lacked sufficient methodological rigour, did not address the substantive governance or sustainability dimensions of the review, or were conceptually redundant. The resulting 48 studies were subjected to the predefined quality-appraisal procedure. At this stage, 18 studies scoring below the minimum threshold of 31 out of 50 were excluded, leaving 30 studies for the final meta-synthesis. The complete screening pathway, including identification, screening, eligibility assessment, quality appraisal, and final inclusion, is presented in Figure 3.

Table 2. Specifications of CASP assessment questions

No.	Question title	Question description
1	Research objectives	Is the selected article aligned with the objectives of your intended research (digital finance governance, cyber resilience, digital trust, and responsible AI)?
2	Up-to-dateness	Are the internal data and information in the article up-to-date (reflecting recent developments in digital financial technologies, cyber threats, and AI advancements)?
3	Research design	How do you evaluate the research design presented in the article?
4	Sampling method	How do you assess the statistical population and selected samples in this article?
5	Data collection	How do you rate the data collection process in this article?
6	Transferability	Can the findings and points in this article be generalised or applied to other contexts (e.g., different countries, various regulatory regimes, differing technological maturity levels)?
7	Ethical considerations	Have ethical principles such as proper referencing, data integrity, and transparency been observed?
8	Data analysis accuracy	To what extent is the data analysis in this article accurate and rigorous?
9	Clarity of findings	How clear and well-articulated are the language and presentation of the article's findings?
10	Research value	What is your overall assessment of the value of this article to the field of digital finance governance, cyber resilience, trust, and responsible AI?

The 739 unique records were assessed sequentially through title screening, abstract screening, and full-text eligibility assessment. Records were excluded only when they failed to satisfy the predefined criteria concerning topical relevance, methodological adequacy, publication type, or substantive engagement with digital finance governance, cyber resilience, digital trust, responsible AI, or sustainable development. Progressively, those investigations that did not correspond to the predefined research questions particularly those focusing on non-digital financial governance, physical (rather than cyber) resilience, trust in non-financial contexts, or AI without an ethical/ responsible approach were systematically removed.

Throughout this procedure, each study was assessed on the basis of its title, abstract, main body, and methodological framework. This iterative refinement ultimately ensured that only the most relevant articles were preserved, from which a final corpus of 30 high-quality studies was extracted. These studies provided the most robust and comprehensive answers to the research questions concerning digital finance governance, cyber resilience dimensions, digital trust components, responsible AI principles, and their linkages with sustainable economic development. Table 3 provides a comprehensive listing of the Selected Articles, detailing their titles alongside the corresponding bibliographic references.

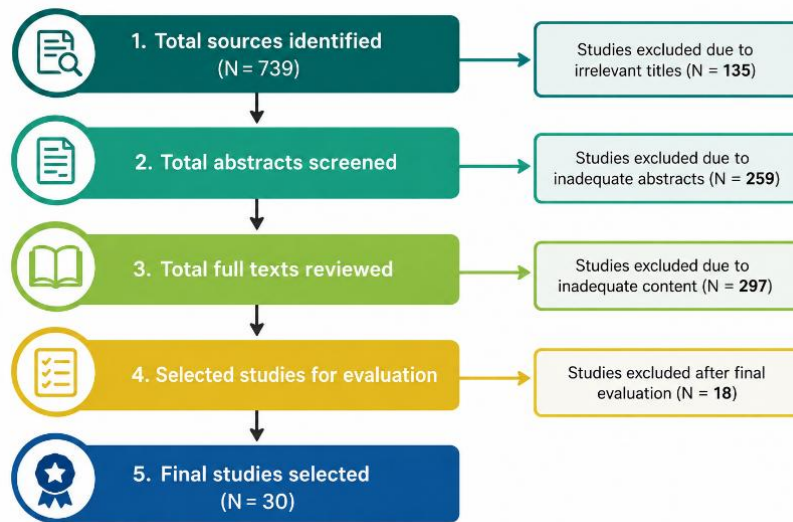


Figure 3. Review and selection process

Table 3. Selected articles

NO.	Title & Source	Research design	Country/Region	Theoretical framework	Quality score
1	Securing financial systems through data sovereignty (Patil et al., 2025)	Systematic literature review	Global	Data sovereignty/ Information security	42 (E)
2	Phishing, vulnerabilities, and AI defense in digital microfinance (Mathenge et al., 2026)	Systematic literature review	Global/ Developing economies	Socio-technical systems / cybersecurity	40 (VG)
3	Digital transformation in achieving SDGs in emerging countries (Atieh et al., 2026)	Quantitative/ Empirical	Emerging economies	Technological capability theory	35 (VG)
4	The nexus between fintech and green finance (Khan & Shahid, 2026)	Systematic literature review	Cross-country	Green finance/ ESG	37 (VG)

NO.	Title & Source	Research design	Country/Region	Theoretical framework	Quality score
5	Digital platforms and crime governance (Shan, 2026)	Qualitative/Case study	China	Platform governance/criminology	39 (VG)
6	Socio-technical foundations of sustainable finance (Neviana et al., 2026)	Bibliometric analysis	Indonesia/Global	Socio-Technical Systems (STS)	41 (E)
7	The impact of FinTech on the UN SDGs (Bahoo et al., 2026)	Hybrid systematic review	Global	SDG/Financial inclusion	42 (E)
8	Role of emerging technologies in SDGs (Fatima & Carè, 2026)	Systematic literature review	Developing countries	Innovation & Sustainability	41 (E)
9	Sustainable financial markets in the digital era (Clim et al., 2026)	Quantitative/Empirical	United Kingdom (UK)	ESG/Market efficiency	34 (VG)
10	Sustainable finance through FinTech (Paul et al., 2026)	Systematic literature review	Global	Sustainable finance	40 (VG)
11	From data jungle to data governance (Volz et al., 2025)	Multi-case study (Qualitative)	Global (Digital ecosystems)	Data governance/Institutional theory	43 (E)
12	Advancing sustainability through financial inclusion (Mamun & László, 2025)	Systematic literature review	Global	Financial inclusion/Sustainability	38 (VG)
13	Toward an evolving framework for responsible AI for credit scoring (Mathen & Paul, 2025)	Systematic literature review	Global	Responsible AI/ Banking ethics	44 (E)
14	Social contract theory & cybersecurity (Kleiner, 2025)	Systematic literature review	Global	Social contract theory	39 (VG)
15	AI governance: A systematic review (Batool et al., 2025)	Systematic literature review	Global	AI governance/Ethics	44 (E)
16	Responsible AI practices in real-world settings (Bach et al., 2025)	Systematic literature review	Global	Responsible AI (RAI)	42 (E)
17	Navigating responsible AI governance (Ferjani et al., 2025)	Systematic literature review	Global	Co-governance/ AI ethics	38 (VG)
18	Who, what, how of RAI governance (Kuehnert et al., 2025)	Meta-Analysis/Review	Global	RAI lifecycle/Actor-network	43 (E)

NO.	Title & Source	Research design	Country/Region	Theoretical framework	Quality score
19	A survey on digital trust (Saveljeva & Volkova, 2025)	Conceptual/Theoretical	Global	Digital trust/Openness	41 (E)
20	AI integration in financial services (Vuković et al., 2025)	Scientometric review	Global	AI governance/Regulation	43 (E)
21	Aligning regulation & governance for cyber resilience (Cojocar, 2025)	Conceptual/Framework	United Kingdom (UK)	Cyber resilience/Regulation	45 (E)
22	Trust in human-AI collaboration in finance (Mirabile et al., 2026)	Bibliometric-systematic review	Global	Trust/ AI governance	42 (E)
23	Digital transformation & financial stability (Hordofa, 2024)	Empirical/Quantitative	Ethiopia (Emerging market)	Financial stability/ Risk	37 (VG)
24	Internet governance & cyber-security (Yusif et al., 2024)	Systematic literature review	Global	Internet governance	39 (VG)
25	Evolution of cyber resilience (Tzavara & Vassiliadis, 2024)	Historical/Conceptual review	Global	Cyber resilience	40 (VG)
26	Trust and security as determinants of fintech adoption in banking (Jafri et al., 2023)	Systematic literature review	Global	Trust and security/ Fintech adoption	39 (VG)
27	ML-driven cybersecurity in digital banks (Asmar & Tuqan, 2024)	Review/Conference paper	Global	Cybersecurity/ Digital banks	38 (VG)
28	Digital governance: Conceptual framework (Hanisch et al., 2023)	Conceptual/Theoretical	Global	Digital governance/ Business research	42 (E)
29	Cyber governance studies (Savaş & Karataş, 2022)	Systematic literature review	Global	Cybersecurity governance	38 (VG)
30	Trust in digital sovereignty (Misra et al., 2025)	Conceptual/Review	Global	Digital sovereignty/ Privacy	37 (VG)

Table 4. Three-level thematic analysis of findings

Second-level constructive theme	First-level constructive theme	Initial theme (Open codes)
Governance of digital finance in cyberspace	Institutional and regulatory frameworks	Regulatory fragmentation across national jurisdictions and its impact on cross-border digital financial services;

Second-level constructive theme	First-level constructive theme	Initial theme (Open codes)
		Data sovereignty and localization requirements (e.g., GDPR, China's Cybersecurity Law, India's data protection framework); Corporate governance adaptation to digital finance: board-level digital oversight, risk committees, and AI governance responsibilities; Policy harmonization efforts for sustainable finance (EU Taxonomy, green bond standards, ESG disclosure regimes); Role of regulatory sandboxes in fostering innovation while maintaining oversight; Supervisory technology (SupTech) for real-time compliance monitoring; Data sovereignty as a critical determinant of cross-border financial data governance, with regulatory fragmentation undermining international coordination.
	Platform-based governance	Digital bureaucracy and state-platform integration in financial services; Governance via mega-platforms (e.g., Alipay, WeChat Pay, M-Pesa) as quasi-regulatory entities; Decentralized governance models in DeFi (automated market makers, DAOs, smart contract governance); Multi-stakeholder governance mechanisms (public-private partnerships, industry self-regulation); Platform accountability for financial crimes (AML/CFT obligations, KYC requirements); Algorithmic governance and the shift from human discretion to automated rule enforcement.
	Cyberspace sovereignty and jurisdictional tensions	Competing state visions for cyberspace governance (US multi-stakeholder vs. China's cyber-sovereignty model); Extra-territorial application of financial regulations (e.g., US sanctions, EU's GDPR reach); Internet governance challenges and the struggle for power among governing bodies; The role of international organizations (IMF, BIS, FATF) in coordinating cross-border financial governance; Multipolar monetary systems and the rise of digital currencies challenging US dollar hegemony;

Cyberspace Studies, Vol 3, No 2, 2022

Second-level constructive theme	First-level constructive theme	Initial theme (Open codes)
Cyber resilience in digital financial systems	Systemic cyber risk management	Cyber diplomacy and statecraft as tools for shaping global financial architecture.
		Cyber resilience as adaptive capacity: ability to anticipate, withstand, recover, and adapt from cyber incidents;
		Systemic cyber risk assessment: modelling contagion effects across interconnected financial infrastructures;
		Cyber risk quantification frameworks (e.g., FAIR model, cyber value-at-risk);
Cyber resilience in digital financial systems	Organizational and operational resilience	Zero-trust security models: continuous verification, least-privilege access, micro-segmentation;
		AI-driven cyber threat detection and response (machine learning for anomaly detection, predictive analytics);
		Cyber resilience maturity models and capability assessment frameworks;
		AI-driven defense mechanisms (e.g., GRU-based mitigation) for addressing phishing and systemic vulnerabilities in digital microfinance institutions.
Cyber resilience in digital financial systems	Regulatory-governance alignment for resilience	Operational resilience mandates in financial regulation (UK PRA/FCA requirements, EU DORA);
		Senior Managers and Certification Regime (SM&CR): individual accountability for cyber risk oversight;
		Red-team testing, cyber-war games, and scenario-based resilience exercises;
		Business continuity planning and disaster recovery for digital financial services;
Cyber resilience in digital financial systems	Regulatory-governance alignment for resilience	Third-party risk management (cloud service providers, fintech partners, outsourcing);
		Institutional learning from cyber incidents and adaptive feedback mechanisms.
		Hybrid supervisory models: combining risk-based, principles-based, and rules-based supervision;
		Regulatory expectations for board-level cyber governance and executive accountability;
Cyber resilience in digital financial systems	Regulatory-governance alignment for resilience	Conductor-oriented oversight vs. box-ticking compliance approaches;
		Adaptive capacity through feedback loops between regulation, governance, and risk engagement;
		Cyber resilience as a continuous process, not a static state;
		Integration of cyber resilience with broader organisational resilience frameworks;

Second-level constructive theme	First-level constructive theme	Initial theme (Open codes)
Digital trust in AI-enabled financial ecosystems	Antecedents and dimensions of digital trust	Structural assurance: technical safeguards, certification, and legal protections; Competence: perceived capability of technology providers and financial institutions; Benevolence: perception that institutions act in users' best interests; Integrity: honesty, transparency, and adherence to ethical standards; Openness: willingness to share information and be transparent about data use; Familiarity and prior positive experience with digital platforms; Privacy and data protection as foundational trust enablers.
	Trust in AI-enabled financial systems	Algorithmic transparency and explainability (XAI) as trust-building mechanisms; Trust calibration: aligning user trust with actual system performance and reliability; Human-AI interaction: anthropomorphism, user interface design, and trust signalling; Trust in automated decision-making (credit scoring, fraud detection, robo-advising); The "black-box" problem and its implications for user trust and regulatory oversight; Trust dynamics across demographic groups (age, digital literacy, cultural differences); The role of third-party auditing and certification in building trust in AI systems; Algorithmic transparency, user interface design, and institutional accountability as joint determinants of trust in human-AI collaboration, with notable demographic variations.
	Trust in digital financial ecosystems	Digital trust as confidence in people, processes, and technology; Trust in sharing economy platforms (peer-to-peer lending, crowdfunding, gig economy); Trust in digital identity systems (self-sovereign identity, biometric verification); Cross-border trust: differences in trust cultures and regulatory regimes; Impact of data breaches and cyber incidents on user trust; Trust repair mechanisms: post-incident

Cyberspace Studies, Vol 3, No 3, 2022

Second-level constructive theme	First-level constructive theme	Initial theme (Open codes)
Responsible Artificial Intelligence (RAI) in finance		transparency, compensation, and communication; Digital trust as a key enabler of fintech adoption and financial inclusion.
		Fairness and bias mitigation: addressing algorithmic discrimination in credit, lending, and insurance; Accountability: clear attribution of responsibility for AI outcomes (human-in-the-loop, human-on-the-loop); Transparency and explainability: making AI decisions understandable to users and regulators; Privacy and data governance: compliance with data protection regulations; AI literacy and capacity building among financial professionals; Human dignity and well-being as central considerations in AI design; Value creation: aligning AI with societal and stakeholder values.
	Ethical and responsible AI principles	Team-level governance: AI ethics committees, review boards, and responsible AI champions; Organization-level governance: AI policies, risk registers, and compliance procedures; Industry-level governance: sector-wide codes of conduct, shared standards, and best practices; National-level governance: AI regulations (EU AI Act, China's AI governance framework, US executive orders); International-level governance: global coordination through OECD, UNESCO, and G7/G20; Regulatory sandboxes for AI testing in financial services; Tools and frameworks for responsible AI implementation (auditing tools, impact assessments).
	AI governance mechanisms and practices	Gap between high-level principles and operational practices in real-world settings; Ad hoc implementation and lack of standardized RAI practices in 80% of deployed AI systems; Lack of stakeholder involvement: underrepresentation of end-users and impacted communities; Tool validation gaps: scarcity of empirically validated responsible AI tools;
	Gaps and challenges in RAI implementation	

Second-level constructive theme	First-level constructive theme	Initial theme (Open codes)
Sustainable economic development through digital finance		Neglect of non-technical roles (organisational leaders, deployers, end-users) in governance design; Lifecycle imbalances: focus on data-centric stages, neglect of value proposition and deployment phases; Co-governance scenarios: envisioning AI as a co-governing partner by 2035; Persistent principle-practice gap in responsible AI for credit scoring, particularly in bias mitigation, explainability, and operational deployment.
	Financial inclusion and digital innovation	FinTech for SDG achievement: mechanism of financial inclusion and access to capital; Digital financial inclusion index and its components (access, usage, quality); Impact of mobile banking, digital payments, and agent banking on underserved populations; Inclusivity challenges: digital divide, gender gaps, rural-urban disparities; Indigenous communities, SMEs, and non-Western perspectives in financial inclusion; Crowdfunding and peer-to-peer lending for entrepreneurship and community development; Financial literacy and digital skills as enablers of inclusive finance.
	Green finance and climate resilience	Green finance instruments: green bonds, green Sukuk, ESG-linked loans, carbon credits; Climate risk integration into financial decision-making (stress testing, scenario analysis); FinTech solutions for green investment (AI for ESG analytics, blockchain for carbon tracking); Renewable energy financing and low-carbon technology deployment; Balancing financial inclusion with environmental sustainability; Green digital infrastructure and sustainable digital transformation; Carbon neutrality goals and financial sector contributions (Net Zero Banking Alliance).
	Socio-technical systems and institutional co-evolution	Socio-technical systems theory: inseparability of technology, actors, and institutions in digital finance; Institutional resilience in digital financial

Cyberspace Studies, Vol 3, No 3, 2022

Second-level constructive theme	First-level constructive theme	Initial theme (Open codes)
		systems: adaptive capacity of regulatory frameworks; Co-evolution of technology, governance, and sustainability outcomes; Digital transformation as a continuous process of socio-technical transition; Tensions between innovation, stability, and sustainability in financial systems; Responsible digital finance: aligning innovation with long-term development goals; Cross-sectoral coordination and multi-stakeholder collaboration for sustainable finance.

(Source: Research findings)

Table 5 presents the frequency distribution of the most recurrent keywords identified across the 30 included studies. The thematic cluster labels are derived from the researchers' interpretive synthesis of keyword patterns during the axial and selective coding phases of the meta-synthesis. This qualitative clustering is intended to provide a high-level thematic overview of the field's major foci, rather than a formal quantitative network analysis. Accordingly, no network visualization software (e.g., VOSviewer or Gephi) was employed, as the primary methodology of this study is a qualitative meta-synthesis, not a bibliometric or scientometric review.

Table 5. Keyword frequency distribution and thematic clustering

Rank	Keyword	Frequency	Co-occurrence cluster
1	Digital finance / FinTech	18	Governance & Innovation
2	Cyber resilience	14	Security & Risk
3	Artificial Intelligence (AI)	13	Technology & Ethics
4	Digital trust	11	Trust & User Acceptance
5	Sustainable development/SDGs	10	Sustainability & Policy
6	Governance	9	Institutional & Regulatory
7	Cybersecurity	8	Security & Risk
8	Financial inclusion	8	Sustainability & Access
9	Responsible AI/ Ethical AI	7	Ethics & Governance
10	Digital transformation	7	Innovation & Change
11	Green finance	6	Sustainability & Investment
12	Data governance	5	Institutional & Regulatory
13	Blockchain	5	Technology & Trust
14	Socio-technical systems	4	Theory & Integration
15	Privacy	4	Trust & Security
16	Risk management	4	Security & Governance
17	Regulatory compliance	3	Governance & Policy
18	Explainability (XAI)	3	Responsible AI
19	Stakeholder involvement	3	Governance & Ethics
20	ESG (Environmental, Social, Governance)	3	Sustainability & Finance

(Source: Research findings)

4.3. Towards a testable theoretical framework: Proposed propositions

While our integrated framework identifies the core components of digital finance governance and their interdependencies, the synthesis also permits the induction of specific, testable propositions that can guide future empirical research. These propositions are not tested by our data but are derived logically from the patterns observed across the 30 reviewed studies. We propose the following:

Proposition 1 (Governance-Resilience Nexus). The effectiveness of cyber resilience strategies in digital financial systems is positively moderated by the degree of regulatory harmonisation and cross-border institutional coordination. In other words, fragmented governance (e.g., conflicting data localisation laws, divergent supervisory frameworks) reduces the marginal utility of technical resilience investments. This proposition follows from the persistent finding that cyber resilience failures often stem from regulatory misalignment rather than technological inadequacy alone.

Proposition 2 (Trust-AI Alignment). User trust in AI-enabled financial services is jointly determined by algorithmic explainability (transparency) and institutional accountability (e.g., third-party auditing, regulatory oversight), and these two factors exhibit a multiplicative (interactive) rather than additive effect on trust formation. That is, explainability without accountability, or accountability without explainability, yields diminishing returns in trust-building- a hypothesis that emerges from the synthesis of digital trust and responsible AI literatures.

Proposition 3 (Sustainability Tension Hypothesis). The relationship between digital financial inclusion and environmental sustainability follows an inverted U-shaped (curvilinear) trajectory: inclusion initially increases carbon emissions due to expanded economic activity and digital infrastructure, but beyond a critical threshold, the greening effects of digital finance (e.g., green bonds, ESG analytics, paperless transactions) offset these initial increases, with the inflection point moderated by the availability of green digital infrastructure. This proposition directly addresses the paradoxical finding in our synthesis (e.g., Kumari et al., 2025) that FinTech inclusion is associated with emissions increases, while other studies show FinTech enabling green finance.

We offer these propositions as a roadmap for future research to move beyond descriptive identification of components toward causal and moderating explanations of how digital finance governance shapes sustainable development outcomes.

5. Discussion

A central finding across the reviewed studies is that governance remains the most contested and challenging dimension. Traditional institutional assumptions of territoriality and centralised authority are increasingly

inadequate for regulating digital financial systems that operate across borderless networks (Teng et al., 2026; Shan, 2026; Yusif et al., 2024). The emergence of platform-based governance evident in both state-platform integration (Shan, 2026) and decentralised finance models reflects a fundamental shift from hierarchical to network-based governance arrangements. However, the literature reveals persistent tensions between multi-stakeholder aspirations and power-driven state-centric approaches (Yusif et al., 2024; Savaş & Karataş, 2022), suggesting that governance solutions must be regionally contextualised while maintaining international coordination. This institutional fragmentation creates regulatory uncertainty that directly undermines both cyber resilience and digital trust. This regulatory uncertainty is further compounded by data sovereignty conflicts; as (Patil et al., 2025) demonstrate, divergent national data governance frameworks undermine the effectiveness of cross-border financial oversight and create operational complexity for multinational fintech institutions.

Cyber resilience has evolved from a technical concern to a strategic systemic imperative. The synthesis confirms that resilience extends beyond cybersecurity to encompass adaptive capacity the ability to anticipate, withstand, recover from, and adapt to cyber incidents (Tzavara & Vassiliadis, 2024; Cojocaru, 2025). Cojocaru's integrative framework connecting regulatory strategy, governance execution, risk engagement, and adaptive feedback provides a valuable model for understanding how institutions build resilience capacity.

However, the literature also reveals a significant divergence: while some studies assume digitalisation automatically enhances stability (Hordofa, 2024), empirical evidence from Ethiopia demonstrates that rapid digital transformation can undermine financial stability when regulatory frameworks and risk management practices lag behind technological change. This paradox underscores that resilience is not an inherent property of digital systems but an emergent outcome of institutional capacity. Extending this institutional perspective (Mathenge et al., 2026), highlight that digital microfinance institutions in developing economies face acute cyber vulnerabilities particularly phishing attacks and argue that AI-driven mitigation strategies, while technologically promising, require simultaneous investment in institutional capacity-building and user awareness to achieve meaningful resilience. Complementing this view (Asmar & Tuqan, 2024), identify that digital banks are particularly vulnerable to a spectrum of sophisticated cyber threats, including insider threats, DDoS assaults, ransomware, phishing, and social engineering, and argue that integrating machine learning algorithms such as SVM, RNN, HMM, and LOF into cybersecurity frameworks is essential for proactive threat detection and prevention.

Furthermore, their proposed model incorporates ethical considerations and leverages a SWOT analysis to balance the strengths

and weaknesses of ML adoption, aiming to fortify system resilience and preserve customer trust within the digital banking ecosystem.

Digital trust emerges as a multidimensional construct that extends traditional trust theories to digital environments. Complementing this view (Jafri et al., 2023), conduct a systematic literature review that synthesizes previous Fintech literature on behavioral intentions in banking, highlighting that trust and security are among the most well-utilized predictors of Fintech adoption, alongside performance expectancy, perceived usefulness, and attitude. Furthermore, their analysis, grounded in the ROSES framework and employing thematic and weight analysis, identifies five primary themes and 24 sub-themes, while also leveraging the TCCM framework to pinpoint research gaps and offer future research directions, ultimately providing valuable insights for Fintech companies and regulatory authorities on the preferred attributes of Fintech services that can enhance adoption within the banking sector (Saveljeva & Volkova, 2025), identification of “openness” as an additional factor complementing ability, benevolence, and integrity significantly advances the conceptualisation of trust in digital finance. Across the literature, trust is consistently framed as confidence in people, processes, and technology, with data protection and privacy serving as foundational enablers (Mirabile et al., 2026; Hidayat-ur-Rehman et al., 2026). This evidence positions digital competence as an indispensable pillar of institutional trust, aligning with the 'competence' dimension of digital trust and highlighting the necessity for financial professionals to possess both domain-specific and technological capabilities. However, the synthesis reveals that digital trust is not uniformly achieved; demographic differences (age, gender, digital literacy) and contextual factors (regulatory regimes, cultural attitudes) create significant heterogeneity in trust formation. This suggests that trust building strategies must be tailored to specific user populations and institutional contexts. Supporting this contextual view (Mirabile et al., 2026), empirically demonstrate that algorithmic transparency and institutional accountability interact multiplicatively in shaping trust, and that trust formation varies significantly across age groups, digital literacy levels, and cultural settings reinforcing the need for differentiated trust-building approaches in AI-enabled financial services.

The responsible AI literature, while rapidly expanding, reveals a critical gap between principles and practice. Despite extensive frameworks and guidelines, Bach et al. (2025) found that almost 80% of AI-enabled systems in high-risk real-world settings (which include, but are not limited to, finance) lack systematic responsible AI practices, highlighting the generalisability of this implementation gap to the financial sector. Batool et al. (2025) and Kuehnert et al. (2025) demonstrate that most available tools focus on technical, data-centric stages, neglecting organisational leaders, end-users, and impacted

communities a significant governance gap. This imbalance reflects a broader tendency toward technological solutionism rather than comprehensive institutional governance. The socio-technical nature of AI governance requires multi-level approaches spanning team, organisation, industry, national, and international levels, yet implementation remains fragmented and ad hoc. This finding aligns with Shahghasemi (2026) critical observation that generative AI systems concentrate epistemic power in the hands of a few technology corporations, necessitating transparent and democratic governance mechanisms to ensure accountability and public trust. This principle-practice gap is particularly pronounced in credit scoring, where Mathen and Paul (2025) find that responsible AI frameworks remain largely aspirational; few institutions have operationalised bias detection, explainability requirements, or stakeholder involvement in their algorithmic decision-making pipelines, reflecting a systemic failure to translate ethical principles into enforceable practices.

Sustainable economic development through digital finance presents both opportunities and tensions. There is strong consensus that FinTech enhances financial inclusion, transparency, and access to capital (Bahoo et al., 2026; Paul et al., 2026), contributing to multiple SDGs. However, the FinTech-green finance nexus is not uniformly positive. Kumari et al. (2025) found that digital financial inclusion in Asian economies is paradoxically associated with increased CO₂ emissions, highlighting the need for green digital infrastructure and sustainability-oriented governance. This tension between financial inclusion and environmental sustainability requires integrated strategies that balance access, innovation, and ecological impact.

The findings of this meta-synthesis carry direct implications for the achievement of specific Sustainable Development Goals (SDGs). First, the emphasis on financial inclusion and access to capital through FinTech directly supports SDG 8 (Decent Work and Economic Growth), as digital finance enables entrepreneurship, job creation, and economic participation among underserved populations (Bahoo et al., 2026; Paul et al., 2026; Meniago, 2025). Second, the focus on cyber resilience and AI-driven infrastructure aligns with SDG 9 (Industry, Innovation, and Infrastructure), as resilient digital financial systems are foundational to sustainable industrial development and technological innovation (Cojocaru, 2025; Tzavara & Vassiliadis, 2024; Fatima & Carè, 2026). Third, the study's central concern with governance, institutional trust, transparency, and accountability directly addresses SDG 16 (Peace, Justice, and Strong Institutions), as effective governance frameworks are essential for reducing corruption, ensuring regulatory compliance, and building public trust in digital financial ecosystems (Yusif et al., 2024; Savaş & Karataş, 2022; Batool et al., 2025; Kuehnert et al., 2025). Finally, the recurring emphasis on multi-stakeholder coordination, cross-sectoral collaboration, and

regulatory harmonization resonates with SDG 17 (Partnerships for the Goals), as no single actor or nation can govern digital finance in isolation (Bahoo et al., 2026; Mamun & László, 2025). These connections underscore that the integrated governance framework proposed in this study is not merely a theoretical exercise but a practical roadmap for advancing sustainable development in the digital age.



Figure 4. Selected sustainable development goals: Goals 8, 9, 16, and 17 (United Nations, 2025)

A critical epistemological qualification is necessary regarding the concept of co-evolution. While our meta-synthesis robustly demonstrates that governance, resilience, trust, and responsible AI are mutually implicated meaning that tensions or advancements in one domain consistently correspond with adaptations in others our data do not permit us to observe these dynamics over time. Co-evolution, properly understood, is a temporal proposition: it asserts that domains change in response to one another across extended periods. The cross-sectional nature of our evidence base (studies published primarily in 2025-2026) cannot establish such temporal causality. Therefore, the co-evolutionary logic we articulate is advanced here as a theoretical proposition and a generative lens for future research, rather than an empirical finding. This framing aligns with the call for longitudinal studies that can trace how governance reforms, cyber incidents, trust shifts, and AI deployments interact over time to shape financial systems.

Points of alignment and divergence across the literature are instructive. Strong agreement exists on the socio-technical nature of digital finance systems, the centrality of governance as the core challenge, and the necessity of multi-level responsible AI governance. However, significant divergence remains on the relationship between digitalisation and stability, the appropriate governance model (multi-stakeholder vs. state-centric), and the conceptualisation of

digital trust. These differences reflect genuine contextual variations geographical, institutional, and technological suggesting that universal governance prescriptions are unlikely to succeed.

Theoretical contributions of this study are threefold. First, it extends institutional theory to cyberspace governance, demonstrating how institutional logics interact in shaping governance outcomes and how institutional voids create space for new governance forms. Second, it advances socio-technical systems theory by demonstrating how governance, resilience, trust, and AI are deeply interdependent and mutually constitutive elements, suggesting a co-evolutionary logic that warrants longitudinal empirical testing. Third, it provides an integrated conceptual framework that addresses the fragmentation characterising existing research, offering a holistic lens for analysing digital finance as a complex adaptive system.

Practically, the findings carry clear implications for policymakers, financial institutions, and technology developers. Regulatory harmonisation, experimental governance through regulatory sandboxes, and board-level accountability for cyber resilience are essential. Institutions must adopt integrated governance frameworks that simultaneously address all five dimensions, moving beyond siloed approaches. Technology developers should prioritise explainability, stakeholder involvement, and validated responsible AI tools across all lifecycle stages.

Future research should focus on cross-contextual comparative studies, empirical investigations of responsible AI implementation, longitudinal and historical analyses that empirically test the proposed co-evolutionary dynamics between governance, resilience, trust, and responsible AI, moving beyond cross-sectional identification of mutual implication toward causal-temporal explanation.

In conclusion, the meta-synthesis confirms that digital finance governance in cyberspace cannot be reduced to technical or regulatory fixes alone. It requires an integrated, adaptive, and context-sensitive approach that recognises the co-evolution of governance, resilience, trust, responsible AI, and sustainability. The framework developed here provides a foundation for navigating this complexity, but its operationalisation demands sustained collaboration across disciplines, sectors, and national boundaries a challenge that defines the next frontier in digital finance research and practice.

6. Conclusion

This meta-synthesis develops an integrated governance framework for digital finance in cyberspace by conceptualising governance, cyber resilience, digital trust, responsible AI, and sustainable economic development as interconnected dimensions of a complex socio-technical system. The synthesis indicates that effective governance cannot be achieved through isolated regulatory interventions or

technical safeguards. Rather, it requires adaptive institutional arrangements capable of coordinating public authorities, financial institutions, technology providers, and affected stakeholders across increasingly borderless digital networks.

The findings further show that cyber resilience is an organisational and institutional capability rather than a purely technical property. Its development depends on regulatory alignment, board-level accountability, risk engagement, continuous learning, and the capacity to anticipate, withstand, recover from, and adapt to cyber incidents. Digital trust similarly extends beyond system functionality. It is constructed through the interaction of technical competence, institutional integrity, structural assurance, transparency, privacy protection, and meaningful user participation.

The analysis also identifies a persistent gap between responsible AI principles and their implementation in financial practice. Addressing this gap requires governance mechanisms that operate across the entire AI lifecycle and assign clear responsibilities to developers, deployers, managers, regulators, and affected users. Explainability, bias mitigation, stakeholder involvement, and independent oversight should therefore be embedded in organisational processes rather than treated as optional technical additions.

Theoretically, the framework extends institutional theory and socio-technical systems theory to the governance of digital finance in cyberspace. It proposes that governance, resilience, trust, responsible AI, and sustainability are mutually implicated dimensions whose relationships should be examined through future longitudinal and comparative research. The proposed co-evolutionary interpretation is offered as a theoretical proposition rather than as an empirically established temporal relationship.

Practically, the findings call for context-sensitive regulatory coordination, integrated cyber-resilience strategies, board-level responsibility for digital and AI-related risks, and stronger mechanisms for stakeholder participation and accountability. Digital finance can contribute to sustainable economic development only when innovation is accompanied by institutional capacity, trustworthy infrastructures, responsible AI practices, and explicit attention to social and environmental consequences.

Conflict of interest

The authors declared no conflicts of interest.

Ethical considerations

The authors have completely considered ethical issues, including informed consent, plagiarism, data fabrication, misconduct, and/or falsification, double publication and/or redundancy, submission, etc. This article was not authored by artificial intelligence.

During the preparation of this manuscript, the authors used DeepSeek, Gemini, and Perplexity solely for language-related assistance, including grammatical proofreading, sentence-level refinement, and improvement of the clarity and fluency of selected passages. These tools were not used to formulate the research questions, design the review protocol, conduct or supplement the literature search, screen or select studies, extract data, perform coding, undertake thematic synthesis, interpret findings, generate results, or compile scientific references. All decisions concerning study eligibility, data extraction, coding, synthesis, interpretation, and citation verification were made and checked by the authors. The authors retain full responsibility for the accuracy, integrity, originality, and transparency of the manuscript.

Data availability

The dataset generated and analyzed during the current study is available from the author on reasonable request.

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

Acknowledgment

The authors would like to express their sincere gratitude and appreciation for the spiritual support, valuable guidance, and continuous encouragement of Dr. Seyed Mehdi Alvani, Dr. Gholamreza Memarzadeh Tehran. Undoubtedly, the profound insight and moral backing of these distinguished professors have played an essential role in conducting and improving this research. The authors also sincerely thank Islamic Azad University, Qazvin Branch, for providing a suitable scientific and academic environment. The authors further gratefully acknowledge the contribution of the two independent external researchers and the third expert reviewer for their diligent work in coding and adjudicating the selected studies, which was instrumental in ensuring the methodological rigor and reliability of this meta synthesis.

References

- Aarab, A.; El Marzouki, A.; Boubker, O. & El Moutaqi, B. (2025). "Integrating AI in public governance: A systematic review". *Digital*. 5(4): 59. <https://doi.org/10.3390/digital5040059>.
- Alahmad, F.A.; Ghouse, G. & Bhatti, M.I. (2026). "AI and fintech synergy: Strengthening financial stability in Islamic and conventional banks". *Journal of Risk and Financial Management*. 19(1): 21. <https://doi.org/10.3390/jrfm19010021>.
- Al-Okaily, M. & Al-Okaily, A. (2025). "Digital transformation and financial innovation as drivers of firm resilience: Evidence from Jordanian financial

- market". *International Journal of Innovation Science*. 1-24. <https://doi.org/10.1108/IJIS-03-2025-0155>.
- Amofa, M.; Arthur, A.; Lamptey, I.H. & Arthur, E. (2026). "The illusion of inclusion: Institutional quality and the shift from symbolic to substantive digital finance". *Fintech and Digital Accounting Review*. 2(1): 65-79. <https://doi.org/10.1108/FDAR-01-2026-0004>.
- Asmar, M. & Tuqan, A. (2024). "Integrating machine learning for sustaining cybersecurity in digital banks". *Heliyon*. 10(17). <https://doi.org/10.1016/j.heliyon.2024.e37571>.
- Atieh, A.A.; Hijazin, A.F.; Alshdaifat, S.M. & Hasan, E.F. (2026). "Digital transformation and technological capabilities in achieving sustainable development goals in emerging countries". *Discover Sustainability*. 7, 383. <https://doi.org/10.1007/s43621-026-02739-3>.
- Bach, T.A.; Kaarstad, M.; Solberg, E. & Babic, A. (2025). "Insights into suggested Responsible AI (RAI) practices in real-world settings: A systematic literature review". *AI and Ethics*. 5: 3185-3232. <https://doi.org/10.1007/s43681-024-00648-7>.
- Bağcı, R.B.; Raja, J.Z. & Gölgeci, I. (2026). "Bridging different institutional logics: The role of institutional work in translating sustainable product-service systems across contexts". *Journal of Business Ethics*. <https://doi.org/10.1007/s10551-026-06281-0>.
- Bagherifam, N.; Naghdi, S.; Ahmadian, V.; Fazlzadeh, A. & Baghalzadeh Shishehgharkhaneh, M. (2025). "Digital regulatory governance: The role of RegTech and SupTech in transforming financial oversight and administrative capacity". *International Journal of Financial Studies*. 13(4). <https://doi.org/10.3390/ijfs13040217>.
- Bahoo, S.; Kondrateva, G.; Khabirov, R.; Goodell, J.W. & Paul, J. (2026). "The impact of FinTech on the achievement of the UN Sustainable Development Goals: A hybrid systematic review". *Business Strategy and the Environment*. 1-23. <https://doi.org/10.1002/bse.71298>.
- Batool, A.; Zowghi, D. & Bano, M. (2025). "AI governance: A systematic literature review". *AI and Ethics*. 5: 3265-3279. <https://doi.org/10.1007/s43681-024-00653-w>.
- Bolton, R. & Foxon, T.J. (2015). "Infrastructure transformation as a socio-technical process Implications for the governance of energy distribution networks in the UK". *Technological Forecasting and Social Change*. 90(Part B): 538-550. <https://doi.org/10.1016/j.techfore.2014.02.017>.
- Clim, L.M.; Mândricel, D.A. & Oncioiu, I. (2026). "Sustainable financial markets in the digital era: FinTech, crowdfunding and ESG-driven market efficiency in the UK". *Sustainability*. 18(2). <https://doi.org/10.3390/su18020973>.
- Cojocaru, A. (2025). "Aligning regulation and governance for cyber resilience: A theoretical framework for the UK financial sector". *Computers & Security*. 157. <https://doi.org/10.1016/j.cose.2025.104627>.
- Dafri, W. & Al-Qaruty, R. (2023). "Challenges and opportunities to enhance digital financial transformation in crisis management". *Social Sciences & Humanities Open*. 8(1). <https://doi.org/10.1016/j.ssaho.2023.100662>.
- Dang, Q. & Li, G. (2026). "Unveiling trust in AI: The interplay of antecedents, consequences, and cultural dynamics". *AI & Society*. 41: 669-692. <https://doi.org/10.1007/s00146-025-02477-6>.
- Danladi, S.; Prasad, M.S.V.; Modibbo, U.M.; Ahmadi, S.A. & Ghasemi, P. (2023). "Attaining sustainable development goals through financial inclusion: Exploring collaborative approaches to fintech adoption in developing economies". *Sustainability*. 15(17). <https://doi.org/10.3390/su151713039>.
- Dionysopoulos, L.; Marra, M. & Urquhart, A. (2024). "Central bank digital currencies: A critical review". *International Review of Financial Analysis*. 91. <https://doi.org/10.1016/j.irfa.2023.103031>.
- Fatima, R. & Carè, R. (2026). "Exploring the role of emerging technologies in advancing sustainable development goals (SDGs) in developing countries: A

- comprehensive review". *Current Opinion in Environmental Sustainability*. 79. <https://doi.org/10.1016/j.cosust.2026.101606>.
- Ferjani, I.; Alzahrani, F.A. & Bouzir, N.M. (2025). "Navigating responsible AI: A systematic review of governance mechanisms and future co-governance scenarios". *Procedia Computer Science*. 270: 4726-4735. <https://doi.org/10.1016/j.procs.2025.09.598>.
- Ferrari, V. (2022). "The platformisation of digital payments: The fabrication of consumer interest in the EU FinTech agenda". *Computer Law & Security Review*. 45. <https://doi.org/10.1016/j.clsr.2022.105687>.
- Fratini, S. (2025). "The sociotechnical politics of digital sovereignty: Frictional infrastructures and the alignment of privacy and geopolitics". *Big Data & Society*. <https://doi.org/10.1177/20539517251400729>.
- Gafsi, N. (2025). "The impact of central bank digital currencies (CBDCs) on global financial systems in the G20 country GVAR approach". *FinTech*. 4(3): 35. <https://doi.org/10.3390/fintech4030035>.
- Galindez-Acosta, J.S. & Giraldo-Huertas, J.J. (2026). "Trust behavior in AI emerges from distrust in humans: A machine learning study on decision-making guidance". *Computers in Human Behavior Reports*. 22. <https://doi.org/10.1016/j.chbr.2026.101024>.
- Ghosh, P. & Golder, U. (2026). "Exploring the effects of FinTech adoption on traditional banking: A systematic literature review on opportunities and challenges". *Digital Business*. 6(1). <https://doi.org/10.1016/j.digbus.2026.100163>.
- Giannitsas, D.; Sun, R. & Baptista, J. (2026). "In artificial intelligence (AI) we (dis)trust? Navigating institutional pressures for automation and augmentation in the implementation of AI in organizations". *Information and Organization*. 36(1). <https://doi.org/10.1016/j.infoandorg.2026.100609>.
- Goldstein, A. & Narayanaswamy, S. (2025). "Managing risk in FinTech: Balancing innovation, regulation and consumer protection". *Journal of Risk Management in Financial Institutions*. 18(3): 219-231. <https://ideas.repec.org/a/aza/rmf/00/y2025v18i3p219-231.html>.
- Hanisch, M.; Goldsby, C.M.; Fabian, N.E. & Oehmichen, J. (2023). "Digital governance: A conceptual framework and research agenda". *Journal of Business Research*. 162. <https://doi.org/10.1016/j.jbusres.2023.113777>.
- Hidayat-ur-Rehman, I.; Alay, H.K.; Deveciyan, M.T.; Akhter, F. & Alzahrani, S. (2026). "Empirical analysis to investigate the relationship between digital sharing economy and digital trust". *Future Business Journal*. 12, 12. <https://doi.org/10.1186/s43093-025-00720-6>.
- Hordofa, D.F. (2024). "Impact of digital transformation on financial stability in emerging markets: Evidence from Ethiopia". *Discover Sustainability*. 5, 309. <https://doi.org/10.1007/s43621-024-00540-8>.
- Hwang, K. (2023). "The relevance of neo-institutionalism for organizational change". *Cogent Social Sciences*. 9(2). <https://doi.org/10.1080/23311886.2023.2284239>.
- Islam, M.S. (2026). "Institutional fragility and cross-border cyber risk in financial systems: Insights from the 2016 Bangladesh Bank heist". *Computers*. 15(7). <https://doi.org/10.3390/computers15070432>.
- Jafri, J.A.; Mohd Amin, S.I.; Abdul Rahman, A. & Mohd Nor, S. (2023). "A systematic literature review of the role of trust and security on Fintech adoption in banking". *Heliyon*. 10(1). <https://doi.org/10.1016/j.heliyon.2023.e22980>.
- Jang, M. (2026). "Building trust in AI: The role of technical capacity, social risk, and corporate institutional accountability". *Information*. 17(2). <https://doi.org/10.3390/info17020212>.
- Jin, X. & Xie, Q. (2024). "The impact of digital transformation on excessive financialization in the real economy". *Sustainability*. 16(23). <https://doi.org/10.3390/su162310464>.
- Kango, U. (2025). "Algorithmic governance". In W. Xu (Ed.). *Handbook of Human-Centered Artificial Intelligence*. Springer. https://doi.org/10.1007/978-981-97-8440-0_90-1.
- Kasarci, I.; Demircan, Z.A.; Ercan, G.Ç. & İnci, T. (2025). "Managing artificial

- intelligence ethics in higher education: A systematic framework for issues and policy recommendations". *International Journal of Current Educational Studies*. 4(2): 1-26. <https://doi.org/10.46328/ijces.223>.
- Khan, I. & Shahid, M.S. (2026). "The nexus between fintech and green finance in advancing sustainable performance across countries". *Discover Sustainability*. 7, 49. <https://doi.org/10.1007/s43621-025-02268-5>.
- Khezri, S.A. & Rezaei, F. (2026). "Mapping the role of blockchain, IoT, and AI in advancing sustainable development goals: A systematic review toward responsible investment. *Knowledge Economy Studies*. 3(2). <https://doi.org/10.22034/kes.2026.2093309.1121>.
- Kim, E.E. (2026). "Ethical AI standards and governance: A perspective of human-centered AI". In W. Xu (Ed.). *Handbook of Human-Centered Artificial Intelligence*. Springer. https://doi.org/10.1007/978-981-97-8440-0_61-2.
- Kleiner, J. (2025). "The social contract theory meets cybersecurity: Systematic literature review". *Digital Policy, Regulation and Governance*. 27(4): 446-465. <https://doi.org/10.1108/DPRG-06-2024-0118>.
- Kuehnert, B.; Kim, R.M.; Forlizzi, J. & Heidari, H. (2025). "The "Who", "What", and "How" of responsible AI governance: A systematic review and meta-analysis of (actor, stage)-specific tools". In *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency (FAccT '25)* (pp. 1–16). ACM. <https://doi.org/10.1145/3715275.3732191>.
- Kumari, D.; Giri, A.K. & Malesios, C. (2025). "Impact of digital financial inclusion on environmental sustainability in Asian economies". *Discover Sustainability*. 6: 1122. <https://doi.org/10.1007/s43621-025-01922-2>.
- Landis, J.R. & Koch, G.G. (1977). "The measurement of observer agreement for categorical data". *Biometrics*. 33(1): 159-174. <https://doi.org/10.2307/2529310>.
- Lawrence, T.B. & Shadnam, M. (2008). "Institutional theory". In *The International Encyclopedia of Communication*. Wiley. <https://doi.org/10.1002/9781405186407.wbieci035>.
- Lendvai, G.F. & Gosztönyi, G. (2025). "Algorithmic bias as a core legal dilemma in the age of artificial intelligence: Conceptual basis and the current state of regulation". *Laws*. 14(3): 41. <https://doi.org/10.3390/laws14030041>.
- Lezzi, M.; Montefusco, P.; Lazoi, M. & Corallo, A. (2025). "AI-based cybersecurity for a sustainable digital industry: Systematic literature review and future research directions". *Journal of Industrial Information Integration*. 48. <https://doi.org/10.1016/j.jii.2025.100980>.
- Li, J. (2026). "Artificial intelligence, ethical amplification, and systemic risk in financial markets". *AI and Ethics*. 6, 367. <https://doi.org/10.1007/s43681-026-01241-w>.
- Lincoln, Y.S. & Guba, E.G. (1985) "Naturalistic inquiry". *SAGE, Thousand Oaks*. 289-331. [http://dx.doi.org/10.1016/0147-1767\(85\)90062-8](http://dx.doi.org/10.1016/0147-1767(85)90062-8).
- Lu, J.; García-Badell, G. & Rodríguez, J.B. (2025). "Digital heritage from a socio-technical systems perspective: Integrated case analysis and framework development". *Heritage*. 8(9). <https://doi.org/10.3390/heritage8090348>.
- Mai, K.L.; Nguyen Thi, N.Q. & Cao, T.H. (2025). "Trust in FinTech: A systematic literature review of key determinants and policy lessons for digital finance in Vietnam". *British Journal of Business Sciences*. 1(1): 12-25. <https://doi.org/10.65687/bjbs.v1i1.2>.
- Mamun, A.Y. & László, V. (2025). "Advancing sustainability through financial inclusion and sustainable finance: A systematic literature review". *Digital Finance*. 7: 853-870. <https://doi.org/10.1007/s42521-025-00142-7>.
- Marak, N.R. & Ayyagari, L.R. (2025). "Artificial intelligence for financial inclusion and sustainable development: A systematic literature review". *Discover Artificial Intelligence*. 5, 390. <https://doi.org/10.1007/s44163-025-00668-0>.
- Mathen, M.P. & Paul, A. (2025). "Toward an evolving framework for responsible AI for credit scoring in the banking industry". *Journal of Information, Communication and Ethics in Society*. 23(1): 148-163.

- <https://doi.org/10.1108/JICES-08-2024-0122>.
- Mathenge, R.; Mukunga, C. & Mwangi, E. (2026). "Phishing, vulnerabilities, and AI defense: A systematic review of cybersecurity challenges and GRU-based mitigation strategies in digital microfinance institutions". *Journal of Cyber Security*. 8: 129-151. <https://doi.org/10.32604/jcs.2026.077183>.
- Meniago, C. (2025). "Digital financial inclusion and economic growth: The moderating role of institutions in SADC countries". *International Journal of Financial Studies*. 13(1): 4. <https://doi.org/10.3390/ijfs13010004>.
- Mirabile, M.; Corazza, G.E. & Alonso-Moral, J.M. (2026). "Trust in human-AI collaboration in finance: A bibliometric-systematic literature review". *AI & Society*. 41: 7625-7654. <https://doi.org/10.1007/s00146-026-03049-y>.
- Misra, S.; Barik, K. & Kvalvik, P. (2025). "Trust in digital sovereignty: A review of security, privacy, and governance challenges". *Public Organization Review*. <https://doi.org/10.1007/s11115-025-00968-0>.
- Mumford, D. & Shires, J. (2023). "Toward a decolonial cybersecurity: Interrogating the racial-epistemic hierarchies that constitute cybersecurity expertise". *Security Studies*. 32(4-5): 622-652. <https://doi.org/10.1080/09636412.2023.2230879>.
- Neviana; Warganegara, D.L. & Prasetyaningtyas, S.W. (2026). "Examining the socio-technical foundations of digital transformation in sustainable finance: Global bibliometric evidence with insights from Indonesia's Bank 5.0 transition". *Frontiers in Sustainability*. 7. <https://doi.org/10.3389/frsus.2026.1804950>.
- Nouis, S.C.; Uren, V. & Jariwala, S. (2025). "Evaluating accountability, transparency, and bias in AI-assisted healthcare decision-making: A qualitative study of healthcare professionals' perspectives in the UK". *BMC Medical Ethics*. 26(1): 89. <https://doi.org/10.1186/s12910-025-01243-z>.
- Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; ... & Moher, D. (2021). "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews". *PLOS Medicine*. 18(3). <https://doi.org/10.1371/journal.pmed.1003583>.
- Papagiannidis, E.; Mikalef, P. & Conboy, K. (2025). "Responsible artificial intelligence governance: A review and research framework". *The Journal of Strategic Information Systems*. 34(2). <https://doi.org/10.1016/j.jsis.2024.101885>.
- Parthasarathy, S. & Panigrahi, P. K. (2026). "From myth to practice: Tracing the rise of responsible AI". *Journal of Psychology and AI*. 2(1). <https://doi.org/10.1080/29974100.2026.2662255>.
- Patil, A.; Mishra, B.; Chockalingam, S.; Misra, S. & Kvalvik, P. (2025). "Securing financial systems through data sovereignty: A systematic review of approaches and regulations". *International Journal of Information Security*. 24, 159. <https://doi.org/10.1007/s10207-025-01074-4>.
- Paul, N.; Jumman, O.H.; Golder, U.; Sultana, F.; Khandoker, M.S.H. & Hossain, M.M. (2026). "Sustainable finance through FinTech: An in-depth review of global trends and insights". *World Development Sustainability*. 9. <https://doi.org/10.1016/j.wds.2026.100336>.
- Perboli, G.; Simionato, N. & Pratali, S. (2025). "Navigating the AI regulatory landscape: Balancing innovation, ethics, and global governance". *Economic and Political Studies*. 13(4): 367-397. <https://doi.org/10.1080/20954816.2025.2569584>.
- Raihan, A. (2024). "A review of the potential opportunities and challenges of the digital economy for sustainability". *Innovation and Green Development*. 3(4). <https://doi.org/10.1016/j.igd.2024.100174>.
- Raihan, A. & Sarker, T. (2026). "Financial mechanisms for advancing environmental sustainability: A comprehensive review". *Green Technology and Sustainability*. 6, 4. <https://doi.org/10.1007/s44173-026-00029-9>.
- Ricciardi Celsi, L. & Zomaya, A.Y. (2025). "Perspectives on managing AI ethics in the digital age". *Information*. 16(4): 318. <https://doi.org/10.3390/info16040318>.
- Salem, M.R.M. (2026). "Digital financial intuition and AI-driven marketing: Enhancing perceived fairness to improve customer retention in Malaysian Islamic banks". *Interdisciplinary Journal of Management Studies (IJMS)*. 19(3): 583-607.

- <https://doi.org/10.22059/ijms.2025.397480.677731>.
- Sandelowski, M. & Barroso, J. (2007) *Handbook for Synthesizing Qualitative Research*. Springer Publishing Company, New York.
- Santos, E. (2026). "The resource infrastructure economy: A systematic review on regime coupling and infrastructural integration in European sustainability transitions". *Sustainability*. 18(13). <https://doi.org/10.3390/su18136579>.
- Sanz Bayón, P. (2025). "Current and future central bank digital currency (CBDC) projects". In C. Pastor Sempere (Ed.). *Governance and Control of Data and Digital Economy in the European Single Market*. (Vol. 71, pp. 283–307). Springer. https://doi.org/10.1007/978-3-031-74889-9_14.
- Sathiskumar, N.N. & Andersen, P.H. (2025). "Tensions in AI-driven digital servitization in the banking industry: A socio-technical view". *International Journal of Bank Marketing*. 1-35. <https://doi.org/10.1108/IJBM-05-2025-0353>.
- Savaş, S. & Karataş, S. (2022). "Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance". *International Cybersecurity Law Review*. 3(1): 7-34. <https://doi.org/10.1365/s43439-021-00045-4>.
- Saveljeva, J. & Volkova, T. (2025). "A survey on digital trust: Towards a validated definition". *Digital*. 5(2): 14. <https://doi.org/10.3390/digital5020014>.
- Shahghasemi, E. (2026). "Minds at stake: Generative AI, epistemic power, and the competition for knowledge". *Journal of Cyberspace Studies*. 10(2): 341-346. <https://doi.org/10.22059/jcss.2026.412464.1242>.
- (2025). "AI; A human future". *Journal of Cyberspace Studies*. 9(1): 145-173. <https://doi.org/10.22059/jcss.2025.389027.1123>.
- Shan, Y. (2026). "Digital platforms and the transformation of crime governance: The organizational regulation crisis of new type cybercrime". *The Journal of Chinese Sociology*. 13(1). <https://doi.org/10.1186/s40711-025-00252-0>.
- Shao, S.P.; Bie, X. & Kim, J.M. (2026). "From digitalization awareness to consumer outcomes: The sequential roles of risk appraisal and platform trust in the Chinese e-commerce context". *Journal of Theoretical and Applied Electronic Commerce Research*. 21(6). <https://doi.org/10.3390/jtaer21060168>.
- Siddik, A.B. & Amin, N.U. (2026). "Disruptive innovation or systemic resilience? Investigating the impact of artificial intelligence on banking stability". *Research in International Business and Finance*. 82. <https://doi.org/10.1016/j.ribaf.2025.103245>.
- Singh, K.; Chatterjee, S.; Mariani, M. & Fosso Wamba, S. (2025). "Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment". *Technovation*. 143. <https://doi.org/10.1016/j.technovation.2025.103219>.
- Tay, L.Y.; Tai, H.T. & Tan, G.S. (2022). "Digital financial inclusion: A gateway to sustainable development". *Heliyon*. 8(6). <https://doi.org/10.1016/j.heliyon.2022.e09766>.
- Teng, H.W.; Hårdle, W.K.; Osterrieder, J.; Pele, D.T.; Baals, L.J.; ... & Xhumari, E. (2026). "Digital assets: Risks, regulations, mitigation". *Financial Innovation*. 12(1): 65. <https://doi.org/10.1186/s40854-025-00848-y>.
- Tzavara, V. & Vassiliadis, S. (2024). "Tracing the evolution of cyber resilience: A historical and conceptual review". *International Journal of Information Security*. 23: 1695-1719. <https://doi.org/10.1007/s10207-023-00811-x>.
- United Nations. (2025). *Sustainable development goals* [Infographic]. <https://www.un.org/sustainabledevelopment/sustainable-development-goals/>.
- Vărzaru, A.B. (2025). "The digital economy and sustainable development goals: A predictive analysis of the interconnection between digitalization and sustainability in EU countries". *Systems*. 13(6): 398. <https://doi.org/10.3390/systems13060398>.
- Vărzaru, A.A. & Bocean, C.G. (2024). "Digital transformation and innovation: The influence of digital technologies on turnover from innovation activities and types of innovation". *Systems*. 12(9): 359. <https://doi.org/10.3390/systems12090359>.
- Vaya-Arboledas, A.; Ferrer-Oliva, M. & Medina-Merodio, J.A. (2025). "Evolution and perspectives in IT governance: A systematic literature review". *Computers*.

- 14(12): 520. <https://doi.org/10.3390/computers14120520>.
- Volz, F.; Münch, C.; Lohmüller, M. & Küffner, C. (2025). "From data jungle to data governance in digital ecosystems: Empirical evidence from a multiple holistic case study". *Journal of Business Research*. 201. <https://doi.org/10.1016/j.jbusres.2025.115747>.
- Vuković, D.B.; Dekpo-Adza, S. & Matović, S. (2025). "AI integration in financial services: a systematic review of trends and regulatory challenges". *Humanities and Social Sciences Communications*. 12, 562. <https://doi.org/10.1057/s41599-025-04850-8>.
- Wafi, I.; Pamuji, S. & Abdul Nasir, M.D. (2026). "Financial technology as a socio-technical entity in the digital financial system: A systematic literature review". *Indonesian Journal of Innovation Multidiscipliner Research*. 4(2): 1-14. <https://doi.org/10.69693/ijim.v4i2.448>.
- Wang, C.; Yin, Y. & Hu, H. (2026). "The rise of algorithmic governance and the dual revolution: Applications, challenges, and governance of artificial intelligence in public administration". *Technology in Society*. 86. <https://doi.org/10.1016/j.techsoc.2026.103264>.
- Webb, H.C. & Sallos, M. (2025). "Navigating cybersecurity challenges in fintech". In K. Tsanis, H.C. Webb, A. Kaddour, & O. David-West (Eds.). *The Palgrave handbook of fintech in Africa and Middle East*. Palgrave Macmillan. https://doi.org/10.1007/978-981-96-6143-5_22.
- World Bank. (2022). *Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy*. <https://doi.org/10.1596/37340>.
- Yusif, S.; Hafeez-Baig, A. & Anachanser, C. (2024). "Internet governance and cybersecurity: A systematic literature review". *Information Security Journal: A Global Perspective*. 33(2): 158-171. <https://doi.org/10.1080/19393555.2023.2268608>.