JASa (Jurnal Akuntansi, Audit dan Sistem Informasi Akuntansi)
ISSN 2550-0732 print / ISSN 2655-8319 online
Vol. 10 No. 2 / August 2026
DOI;10.36555/jasa.v10i2.3071

Blockchain and Smart Contracts in Modern Auditing: A Systematic Review

Andi Rosyandi Cardiman[1], Agus Widarsono[1]
Universitas Pendidikan Indonesia, Indonesia[1]
*Coresponding Email : andicardiman@upi.edu

ABSTRACT

This study conducts a systematic literature review (SLR) to examine the role of blockchain and smart contracts in modern auditing practice. Following the PRISMA 2020 protocol, 35 peer reviewed articles published between 2016 and 2025 were identified across Scopus, Web of Science, EBSCOhost, and Google Scholar, screened, appraised with the Mixed Methods Appraisal Tool, and analyzed through NVivo assisted thematic synthesis. The review finds that blockchain and smart contracts primarily support continuous auditing, autonomous verification of digital assets, automated internal control monitoring, and privacy preserving financial reporting, while unresolved technical vulnerabilities, the oracle problem, scalability limits, absent audit standard guidance, and an acute auditor skills gap continue to constrain adoption. Agency theory dominates the theoretical landscape, though contract, complexity, and legitimacy theories remain underused. These findings imply that standard setters such as IAASB and PCAOB need blockchain specific guidance, and that audit curricula must be reformed to build blockchain literacy, while firms should treat adoption as contingent on technical maturity, regulatory readiness, and human capital rather than a universal remedy. Unlike prior bibliometric or narrative reviews, this study integrates technical, theoretical, and empirical clusters of literature into a single PRISMA based synthesis and proposes an integrative model in which audit quality gains from blockchain depend jointly on technological maturity, regulatory adequacy, and auditor competence.

ARTICLE INFO

Article history:
Submitted: 27 July 2026
Revised: 21 August 2026
Accepted: 26 August 2026
Published: 30 August 2026

Keyword:
Blockchain
Smart Contracts
Auditing
Systematic Literature Review
Audit quality

To cite this article (APA Style): Cardiman, A. R., & Widarsono, A. (2025). Blockchain and Smart Contracts in Modern Auditing: A Systematic Review. JASa : Jurnal Akuntansi, Audit dan Sistem Informasi Akuntansi. Vol (No), p.336-346. https://doi.org/10.36555/jasa.v10i2.3071

INTRODUCTION

Rapid digital transformation over the past two decades has reshaped global business practice, including financial reporting and assurance services. Blockchain and smart contracts have emerged as among the most disruptive innovations with the potential to redefine the frameworks, methodologies, and standards of modern auditing (Bonsón & Bednárová, 2019; Schmitz & Leoni, 2019). Blockchain a distributed, immutable, and cryptographically secured ledger fundamentally shifts how financial transactions are recorded, validated, and verified by removing dependence on a single trusted intermediary, thereby strengthening data integrity (Christidis & Devetsikiotis, 2016; Lombardi et al., 2022). Complementing this infrastructure, smart contracts are self executing agreements coded directly onto a blockchain that automatically enforce predefined rules without third party intervention, enabling continuous, real time transaction monitoring and reducing audit latency and cost (Ante, 2021; Rozario & Thomas, 2019). Traditional auditing, by contrast, remains periodic and retrospective, relying heavily on sampling and manual verification that are inherently vulnerable to human error, fraud, and information asymmetry (Dai & Vasarhelyi, 2017) a limitation made visible by major accounting scandals from Enron and WorldCom to Wirecard (Cao et al., 2024).

Yet blockchain's promise as a remedy for these vulnerabilities warrants closer scrutiny, since cryptographic immutability guarantees only that a recorded transaction cannot be altered after the fact; it does not verify that the information entered onto the ledger was accurate, complete, or free of manipulation in the first place. This limitation becomes acute wherever smart contracts rely on oracles to import external data such as market prices, shipment status, or third party confirmations, a dependency that malicious actors have repeatedly exploited in practice. Chainalysis documented 41 separate oracle manipulation attacks that drained more than USD 400 million from decentralized finance protocols in 2022 alone, including the USD 117 million exploit of Mango Markets, in which an attacker artificially inflated a token's price to borrow far beyond the platform's genuine collateral value (Chainalysis, 2023). Such incidents demonstrate that blockchain based systems can preserve a permanent, tamper evident record of a transaction while still transmitting false or manipulated information into that record, underscoring that technological immutability alone does not equate to information reliability or audit assurance. This gap between cryptographic trust and substantive truth, alongside the persistence of large scale financial misstatement even in technologically sophisticated environments, is precisely the phenomenon that motivates a systematic review of how the auditing literature has engaged with blockchain's actual, rather than assumed, implications for audit quality.

Academic interest in blockchain enabled auditing has grown exponentially, with bibliometric analyses documenting an acceleration of publications since 2017 (Abu Huson et al., 2024; Secinaro et al., 2021) and literature syntheses concluding that blockchain and artificial intelligence collectively can improve audit quality, mitigate fraud risk, and strengthen financial reporting reliability (Han et al., 2023; Hassanein et al., 2025). Yet, as Bellucci et al., (2024) note, the literature remains fragmented: most studies examine isolated technical, managerial, or regulatory facets of blockchain adoption without integrating them into a comprehensive, systematic framework. Existing reviews are predominantly thematic or bibliometric rather than methodologically systematic, so rigorous PRISMA based syntheses of blockchain auditing research remain scarce (Silva et al., 2022).

Several critical gaps persist. The specific role of smart contracts as autonomous audit instruments, including the oracle problem identified by Sheldon (2021), remains underexplored; regulatory and institutional dimensions of adoption are only partially addressed (Anis, 2023; Tušek et al., 2021); research overwhelmingly focuses on developed economies while developing-country perspectives remain scarce, with Qader and Cek's (2024) Turkish study a rare exception; and the integration of blockchain auditing research with relevant theory agency, signaling, institutional, and innovation diffusion theory remains underdeveloped (Ziemba et al., 2025). Addressing these gaps through a rigorous, theory informed systematic synthesis constitutes the novelty of this study.

This study therefore conducts a systematic literature review, guided by the PRISMA 2020 framework, to map the intellectual landscape of blockchain auditing research, identify the main applications, benefits, and limitations reported in the literature, assess the technical, institutional, and regulatory challenges affecting adoption, examine the theoretical foundations used across studies, and propose a future research agenda. Specifically, the review addresses four research questions: (RQ1) How has research on blockchain and smart contracts in auditing evolved temporally, geographically, and thematically? (RQ2) What applications, benefits, and limitations have been documented? (RQ3) What factors facilitate or hinder adoption across institutional and regulatory contexts? (RQ4) What future research agenda is most urgently needed to close remaining gaps in the literature?

METHODS

This study adopts a Systematic Literature Review (SLR) design following the PRISMA 2020 guidelines (Page et al., 2021) chosen because the blockchain auditing literature is fragmented and heterogeneous, and because a systematic protocol offers more reliable and replicable synthesis than narrative or bibliometric reviews (Tranfield et al., 2003, as cited in Lombardi et al., 2022; Ziemba et al., 2025).

Literature was searched across Scopus, Web of Science, EBSCOhost, and Google Scholar using the Boolean string ("blockchain" OR "distributed ledger" OR "DLT") AND ("smart contract*" OR "self executing contract*") AND ("audit*" OR "assurance" OR "accounting" OR "financial reporting"), applied to title, abstract, and keyword fields, and supplemented by backward/forward citation searching and hand searching of key accounting technology journals. The search was restricted to publications from 2016 to 2025, reflecting the 2015 launch of Ethereum and the resulting surge in blockchain auditing scholarship, though selected foundational pre 2016 works were retained as contextual references.

Studies were included if they substantively addressed blockchain and/or smart contracts within an auditing, accounting, or assurance context; were peer reviewed journal articles, conference proceedings, or academic book chapters published in English or Indonesian between 2016 and 2025; and met a minimum methodological quality threshold assessed with the Mixed Methods Appraisal Tool (MMAT 2018) or, for reviews, AMSTAR 2. Two researchers independently screened records at each PRISMA stage identification, title/abstract screening, full text eligibility, and inclusion resolving disagreements by consensus (Cohen's $\kappa \geq 0.70$). Table 1 summarizes the outcome of each selection phase.

Table 1. PRISMA 2020 Selection Process

Phase	Records	Note
Identification (4 databases)	847	Before deduplication
After deduplication	612	235 duplicates removed
Title/abstract screening	198	414 excluded
Full-text retrieval	167	31 not accessible
Eligibility assessment	89	78 excluded (off topic/low quality)
Additional searches	22	Backward/forward citation + hand search
Final studies included	35	Corpus for data extraction and synthesis

Source: Adapted from Page et al. (2021)

A standardized extraction form captured bibliographic details, study objectives, theoretical grounding, methodology, and substantive findings on blockchain/smart contract applications, benefits, and challenges, piloted on five randomly selected studies before being applied to the full corpus. Thematic synthesis followed Thomas and Harden's (2008, as cited in Bellucci et al., 2024) three stage approach line by line coding, descriptive theme development, and analytic theme construction conducted in NVivo 12, combining deductive coding guided by the research questions with inductive, data driven coding. Risk of bias was assessed at both the individual study level and the synthesis level, including a search for grey literature to gauge publication bias.

RESULTS AND DISCUSSION

Bibliographic Profile and Distribution of Studies

The bibliometric profile of the 35 included studies reveals a pattern of pronounced

growth in blockchain auditing scholarship between 2016 and 2025, corroborating Secinaro et al.'s (2021) thesis of exponential publication growth since 2017. Table 2 summarizes this temporal distribution, showing a shift from a small foundational cohort (2016–2017) toward a mature phase (2022–2025) in which systematic reviews and multi country empirical studies dominate.

Table 2. Temporal Distribution of Included Studies (2016–2025)

Period	Studies	%	Dominant characteristics
2016–2017	2	5.7%	Foundational conceptualization (Christidis & Devetsikiotis, 2016; Dai & Vasarhelyi, 2017)
2018–2019	5	14.3%	Theoretical framework development (Rozario & Thomas, 2019; Schmitz & Leoni, 2019)
2020–2021	10	28.6%	Expansion; first empirical studies (Pimentel et al., 2021; Sheldon, 2021)
2022–2023	11	31.4%	Consolidation; SLRs and multi country studies (Han et al., 2023; Silva et al., 2022)
2024–2025	7	20.0%	Maturation; regulation and AI blockchain integration (Cao et al., 2024; Ziemba et al., 2025)
Total	35	100%	Cumulative growth of 3,400% from 2016–17 to 2022–25

Geographically, production is concentrated in North America (37.1%) and Europe (28.6%), with Asia, the Middle East/North Africa, and other developing regions together accounting for less than a quarter of the corpus (Table 3). This concentration signals a potential geographic bias: findings largely reflect the institutional, regulatory, and professional contexts of developed economies, while Southeast Asia including Indonesia remains conspicuously under represented, a limitation also flagged by Hassanein et al., (2025).

Table 3. Geographic Distribution of Included Studies

Region	Studies	%
United States / Canada	13	37.1%
Europe (multi-country)	10	28.6%
Australia / Oceania	3	8.6%
East Asia (China, Korea)	3	8.6%
Middle East / North Africa	2	5.7%
International (multi-country)	4	11.4%
Total	35	100%

Methodological Profile

Methodologically, the corpus is dominated by conceptual/theoretical papers (31.4%) and systematic reviews (25.7%), followed by bibliometric analyses (14.3%), quantitative surveys (14.3%), qualitative studies (8.6%), and mixed-methods designs (5.7%) (Table 4). This distribution indicates that the evidence base is still being built: most empirical claims rest on cross sectional designs with modest samples, and Han et al. (2023) explicitly flag the scarcity of longitudinal empirical work as a major limitation. Quality appraisal using MMAT 2018 showed that 74.3% of studies (26 of 35) scored 70% or higher, and the

remainder scored between 60–69%, above the inclusion threshold of 60%.

Table 4. Research Design of Included Studies

Design	Studies	%
Conceptual / theoretical paper	11	31.4%
Systematic literature review	9	25.7%
Bibliometric analysis	5	14.3%
Quantitative survey	5	14.3%
Qualitative study	3	8.6%
Mixed methods	2	5.7%
Total	35	100%

Applications of Blockchain and Smart Contracts in Auditing

Thirty two of the 35 studies (91.4%) identify at least one concrete application of blockchain or smart contracts in auditing, clustering into four domains: continuous auditing, autonomous audit instruments, digital asset verification, and privacy preserving financial reporting (Table 5).

Continuous auditing is the most consistently discussed application. Dai & Vasarhelyi, (2017) laid the conceptual foundation by proposing blockchain as an infrastructure for triple entry accounting, in which each transaction is simultaneously recorded by both counterparties and the network itself, inherently producing a tamper resistant audit trail. Building on this, Rozario & Thomas (2019) proposed an "Audit 4.0" framework restructuring three core components of the audit process: real time monitoring replacing sampling, automated verification through smart contracts, and instant reporting. Dong & Pan (2023) empirical study of 248 Chinese firms confirmed the feasibility of this framework, finding that firms integrating blockchain into internal audit functions reduced average anomaly detection time from 47 to 3 days. Sheldon (2022) further distinguished three functional layers Continuous Control Monitoring, Continuous Data Assurance, and Continuous Risk Assessment each requiring distinct technical design and audit competencies.

Rozario & Vasarhelyi (2018) were among the first to conceptualize smart contracts not merely as contract execution mechanisms but as autonomous audit agents capable of confirming third party balances, verifying subsequent events, testing loan covenant compliance, and generating cryptographic audit evidence without human intervention. De Andrés & Lorca (2021) extended this by identifying five areas of substantive procedure transformation: automated third party confirmation, cut off testing rendered largely moot by cryptographic timestamping, full population transaction tracing, on chain ownership vouching, and automated inter party reconciliation.

Pimentel et al. (2021) systematized the challenges of auditing blockchain based assets cryptocurrencies, digital tokens, and tokenized assets arguing that fundamental audit assertions (existence, ownership, valuation, completeness, and presentation) require substantial methodological adaptation, particularly given that ownership verification depends on understanding asymmetric cryptography and private key management, competencies well beyond conventional auditor training. Cao et al. (2024), publishing in Management Science, developed a formal secure multiparty computation model allowing multiple auditors to jointly verify blockchain stored financial data without any party accessing others' raw data an innovation with significant implications for multi client and consortium blockchain audits.

Direct empirical evidence on audit quality is more limited but informative. Qader & Cek (2024), surveying 214 auditors and financial managers in Turkey, found that perceived audit quality increased significantly among blockchain adopting organizations (β = 0.412, p < .001), with data integrity (β = 0.389) and objectivity (β = 0.341) as the strongest contributors, consistent with Bonsón and Bednárová's (2019) argument that blockchain's inherent transparency strengthens auditor independence. Conversely, (Dai & Vasarhelyi, 2017; Dong & Pan, 2023; Hassanein et al., 2025; Rozario & Thomas, 2019) warn of a new threat to audit quality automation bias the tendency to over rely on blockchain system outputs without questioning underlying assumptions, underscoring the need for professional standards that explicitly bound the use of technology in audit judgment.

Table 5. Summary of Blockchain and Smart Contract Applications in Auditing

Domain	Mechanism	Reported benefit	Key references
Continuous auditing	Real-time monitoring of the full transaction population	Faster fraud detection; 100% coverage vs. sampling	(Dai & Vasarhelyi, 2017; Dong & Pan, 2023; Rozario & Thomas, 2019);
Smart contracts as audit agents	Automated execution of verification procedures; instant anomaly alerts	Lower labor cost; elimination of manual procedures	(De Andrés & Lorca, 2021; Rozario & Vasarhelyi, 2018);
Digital asset verification	On chain proof of ownership; asymmetric cryptography	Certainty of existence/ownership; irreversible audit trail	(Pimentel et al., 2021); Sheldon (2021)
Automated internal control	CCM, CDA, CRA via smart contracts	Continuous compliance monitoring without manual intervention	(Bonyuet, 2020; Sheldon, 2022)
Verified financial reporting	Secure multiparty computation + distributed ledger	Data privacy preserved while enabling external verification	(Cao et al., 2024; Han et al., 2023)

Challenges and Barriers to Adoption

All 35 studies identify at least one barrier to adoption, spanning technical technological, institutional regulatory, and human resource levels (Table 6).

Vacca et al. (2021) document four categories of technical vulnerability with direct implications for audit reliability: reentrancy vulnerabilities (dramatically illustrated by the 2016 DAO Hack, which caused losses of approximately USD 60 million), integer overflow/underflow, timestamp dependence exploitable by validators, and front running by parties with privileged access to pending transactions. Sheldon (2021) identifies the oracle problem blockchain's inherent inability to independently verify external, off chain data such as market prices or shipment status as the most fundamental vulnerability, arguing that auditors need dedicated procedures for evaluating oracle reliability, a domain where professional guidance is still absent. Scalability compounds these issues: public blockchains such as Ethereum process only 15–30 transactions per second versus Visa's 24,000+ TPS, limiting feasibility for high volume enterprises, and layer 2 solutions such as Optimism and Polygon remain immature (Dong & Pan, 2023; Vacca et al., 2021).

Tušek et al. (2021) show that current International Standards on Auditing provide no explicit guidance on evaluating oracle reliability, auditing smart contract code, assessing cryptographic risk, or determining materiality in immutable systems a standards gap that creates methodological uncertainty for firms bearing professional and legal responsibility for their opinions. Secinaro et al. (2021) add that cross jurisdictional regulatory disharmony

regarding the legal status of smart contracts, digital signatures, and digital asset taxation compounds the complexity of auditing multinational entities, while Anis (2023) finds that in Egypt this uncertainty is compounded by inadequate technology infrastructure.

The most consistent finding across the literature is an acute skills gap. Han et al. (2023) describe a competency paradox: blockchain can automate many routine audit tasks even as it demands far higher technical competence in smart contract design, consensus protocol security, and blockchain data interpretation than most auditors currently possess. Alshurafat et al. (2023) warn that if the profession fails to adapt quickly, non traditional, technology based assurance providers may erode the position of conventional audit firms.

Table 6. Matrix of Adoption Barriers

Level	Specific barrier	Severity	Key references
Technical	Smart contract vulnerabilities (reentrancy, overflow)	High	(Sheldon, 2021; Vacca et al., 2021)
Technical	Oracle problem: off chain data integrity	Very high	(Rozario & Thomas, 2019; Sheldon, 2021)
Technical	Scalability and throughput limits	Medium	(Dong & Pan, 2023; Vacca et al., 2021)
Technical	Immutability: no post deployment correction	High	(Maffei et al., 2021; Vacca et al., 2021)
Regulatory	Absence of blockchain specific ISA guidance	Very high	(Secinaro et al., 2021; Tušek et al., 2021)
Regulatory	Cross jurisdictional regulatory disharmony	High	(Anis, 2023; Ziemba et al., 2025)
Human resources	Blockchain/cryptography skills gap	Very high	(Alshurafat et al., 2023; Han et al., 2023)
Human resources	Automation bias; erosion of professional skepticism	High	(Han et al., 2023; Hassanein et al., 2025)
Institutional	Resistance to change within conventional firms	Medium	(Anis, 2023; Ziemba et al., 2025)

Theoretical Foundations and Adoption Factors

Agency theory is the dominant lens, applied in 48.6% of studies (17 of 35), followed by innovation diffusion theory (22.9%), institutional theory (17.1%), and signaling theory (14.3%); the remainder adopt a multi theoretical or purely descriptive approach. Agency theory's dominance reflects the field's framing of blockchain as a remedy for the information asymmetry and agency costs that motivate auditing itself: Lombardi et al. (2022) argue blockchain reduces agency costs by providing real time transparency, though they caution that on chain verification does not resolve deeper agency problems such as data manipulation prior to blockchain entry. Three theoretical gaps stand out: the underuse of contract theory and property rights theory highly relevant to the legal and economic implications of smart contracts complexity theory for analyzing blockchain ecosystems' emergent, non linear behavior, and legitimacy theory for explaining firms' adoption motives.

Adoption is shaped by a hierarchy of factors. At the macro level, regulatory pressure and capital market transparency demands are the strongest drivers, followed at the meso level by inter firm competition, and at the micro level by management awareness and IT infrastructure (Ziemba et al., 2025). Firm size moderates these effects: Dong & Pan (2023) find substantially larger benefits for large, high transaction volume firms (β = 0.487) than

for small firms (β = 0.182, p < .01), indicating meaningful economies of scale. Conversely, Anis (2023) application of Rogers' diffusion of innovation theory in Egypt shows that perceived complexity, limited observability of benefits, and incompatibility with existing professional infrastructure most inhibit adoption in developing economies a pattern with clear relevance to other developing contexts, including Indonesia.

Future Research Agenda

Twenty nine of the 35 studies (82.9%) propose future research directions, converging on six priorities (Table 7): longitudinal empirical studies of blockchain's impact on audit quality; development of blockchain specific international audit standards; research situated in developing country contexts; technical and policy solutions to the oracle problem; auditor competency and curriculum transformation; and AI blockchain integration in auditing.

Table 7. Future Research Priorities

Priority	Support	Representative references
Longitudinal studies of audit quality impact	24/35 (68.6%)	(Bellucci et al., 2024; Han et al., 2023; Lombardi et al., 2022)
Blockchain specific international audit standards	21/35 (60.0%)	(Sheldon, 2022; Tušek et al., 2021; Ziemba et al., 2025)
Developing country contexts	18/35 (51.4%)	(Anis, 2023; Hassanein et al., 2025)
Oracle problem: technical/policy solutions	16/35 (45.7%)	(Rozario & Thomas, 2019; Sheldon, 2021)
Auditor competency and curriculum reform	14/35 (40.0%)	(Alshurafat et al., 2023; Han et al., 2023)
AI blockchain integration	12/35 (34.3%)	(Abu Huson et al., 2024; Han et al., 2023)

Integrative Discussion

Synthesizing across clusters, three insights emerge. First, the relationship between blockchain adoption and audit quality improvement is not linear or deterministic; it is conditioned by technical maturity (oracle design, smart contract security), institutional factors (regulatory frameworks, professional standards), and human capital (auditor competence, training, attitudes toward innovation). Blockchain is therefore not a universal remedy for conventional audit limitations its effectiveness depends on implementation quality and adoption context.

Second, an inherent trade off exists between blockchain's transparency and immutability, which strengthen verifiability, and auditors' ethical obligation of client confidentiality; Cao et al. (2024) secure multiparty computation model is among the most promising responses, though its technical complexity limits near term adoption. Third, timing of adoption carries strategic weight: firms delaying adoption risk losing competitive position to technology native entrants (Alshurafat et al., 2023; Ziemba et al., 2025), while premature adoption ahead of mature standards and regulation carries legal and reputational risk. Overall, realizing blockchain's potential to enhance audit quality, efficiency, and integrity requires three conditions to hold simultaneously mature and secure technical implementation, adequate regulatory and professional standards, and audit workforce readiness and the absence of any one condition substantially limits the benefits that can be realized.

These insights directly address the research problem motivating this review:

technological immutability does not, by itself, guarantee the truthfulness of the information a blockchain records. Across the 35 studies synthesized, the oracle problem recurs not as an isolated technical footnote but as a structural vulnerability documented from the earliest conceptual papers through the most recent empirical work, confirming that the verification gap illustrated by real world oracle manipulation incidents remains largely unaddressed by current audit guidance, professional standards, and practitioner competence. Blockchain therefore strengthens the reliability of records once data has entered the ledger, but it does not, on its own, resolve the prior and more fundamental audit question of whether that data was true to begin with.

CONCLUSION

This systematic review of 35 studies published between 2016 and 2025 answers the four research questions guiding this study. In response to RQ1, on how research has evolved temporally, geographically, and thematically, the field has grown from a small foundational cohort of conceptual papers into a maturing body of systematic reviews and multi country empirical studies, though production remains concentrated in North America and Europe, leaving Southeast Asia, including Indonesia, markedly underrepresented. In response to RQ2, on the applications, benefits, and limitations documented in the literature, blockchain and smart contracts are reshaping auditing primarily through continuous, full population monitoring, autonomous verification via smart contracts, and privacy preserving multiparty verification of financial data, while persistent technical vulnerabilities, the unresolved oracle problem, absent blockchain specific audit standards, and a severe auditor skills gap continue to constrain adoption.

In response to RQ3, on the factors that facilitate or hinder adoption across institutional and regulatory contexts, the evidence shows that no single factor determines outcomes: technical maturity, regulatory adequacy, and auditor competence must be present jointly, and the absence of any one condition substantially limits the audit quality benefits that can be realized. Compared with prior thematic and bibliometric reviews, which mapped isolated technical, managerial, or regulatory facets of the literature, this PRISMA based synthesis integrates technical, theoretical, and empirical clusters into a single, replicable framework and shows that agency theory dominates the field's theoretical grounding while contract, complexity, and legitimacy theories remain underused, a gap not previously articulated as clearly in the literature.

In response to RQ4, on the future research agenda most urgently needed, this review identifies three priorities: longitudinal empirical designs capable of tracing audit quality effects over time; studies situated in developing country contexts, including Indonesia, where infrastructure, regulatory capacity, and professional maturity differ meaningfully from the developed economy settings that dominate the current evidence base; and greater theoretical engagement with contract, complexity, and legitimacy theory alongside the currently dominant agency theoretic lens.

These findings carry clear implications. Audit standard setters, particularly IAASB and PCAOB, need evidence based, blockchain specific guidance covering oracle evaluation, smart contract auditing, and materiality in immutable systems; accounting curricula and professional development programs must be reformed to close the blockchain skills gap; and audit firms should treat blockchain adoption as contingent on the joint readiness of technology, regulation, and human capital rather than as a guaranteed source of audit quality improvement.

REFERENCES

Abu Huson, Y., Sierra-García, L., & Garcia-Benau, M. A. (2024). A bibliometric review of information technology, artificial intelligence, and blockchain on auditing. *Total Quality Management & Business Excellence*, *35*(1–2), 91–113. https://doi.org/10.1080/09026519.2023.2249621

Alshurafat, H., Alsmadi, S. A., Alrawad, M., & Alshboul, O. (2023). Navigating the future: Blockchain's impact on accounting and auditing practices. *Sustainability*, *15*(24), 16887. https://doi.org/10.3390/su152416887

Anis, A. (2023). Blockchain in accounting and auditing: Unveiling challenges and unleashing opportunities for digital transformation in Egypt. *Journal of Humanities and Applied Social Sciences*, *5*(4), 359–380. https://doi.org/10.1108/JHASS-06-2023-0072

Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519. https://doi.org/10.1016/j.tele.2020.101519

Bellucci, M., Ciacchini, L., Fiorani, G., & Manetti, G. (2024). Blockchain for accounting and auditing: A systematic literature review. *Journal of Risk and Financial Management*, *17*(7), 276. https://doi.org/10.3390/jrfm17070276

Bonsón, E., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research*, *27*(5), 725–740. https://doi.org/10.1108/MEDAR-11-2018-0406

Chainalysis. (2023). Oracle manipulation attacks rising: A unique concern for DeFi. *Chainalysis Blog*. https://www.chainalysis.com/blog/oracle-manipulation-attacks-rising/

Bonyuet, D. (2020). Overview and impact of blockchain on auditing. *The International Journal of Digital Accounting Research*, *20*, 31–43. https://doi.org/10.4192/1577-8517-v20_2

Cao, S. S., Cong, L. W., & Yang, B. (2024). Distributed ledgers and secure multiparty computation for financial reporting and auditing. *Management Science*, *71*(5), 3852–3872. https://doi.org/10.1287/mnsc.2023.02577

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, *31*(3), 5–21. https://doi.org/10.2308/isys-51804

De Andrés, P., & Lorca, P. (2021). Smart contracts and auditing. *The International Journal of Digital Accounting Research*, *21*, 157–183. https://doi.org/10.4192/1577-8517-v21_6

Dong, Y., & Pan, H. (2023). Enterprise audits and blockchain technology. *SAGE Open*, *13*(4). https://doi.org/10.1177/21582440231218839

Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial intelligence: A literature review. *International Journal of Accounting Information Systems*, *48*, 100598. https://doi.org/10.1016/j.accinf.2022.100598

Hassanein, A., Benameur, K. B., Mostafa, M. M., Al-Shattarat, W., & Magar, N. H. (2025). Mapping the scientific research of blockchain technology in accounting and auditing: Bibliometric analyses and a roadmap for future research. *Cogent Business & Management*, *12*(1). https://doi.org/10.1080/23311975.2025.2513638

Lombardi, R., de Villiers, C., Moscariello, N., & Pizzo, M. (2022). The disruption of blockchain in auditing: A systematic literature review and an agenda for future research. *Accounting, Auditing & Accountability Journal*, *35*(7), 1534–1565. https://doi.org/10.1108/AAAJ-10-2020-4992

Maffei, M., Casciello, R., & Meucci, F. (2021). Blockchain technology: Uninvestigated issues emerging from an integrated view within accounting and auditing practices. *Journal of Organizational Change Management*, *34*(2), 462–476. https://doi.org/10.1108/JOCM-09-2020-0264

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*, n71. https://doi.org/10.1136/bmj.n71

Pimentel, E., Boulianne, E., Eskandari, S., & Clark, J. (2021). Systematizing the challenges of auditing blockchain-based assets. *Journal of Information Systems*, *35*(1), 61–75. https://doi.org/10.2308/ISYS-19-007

Qader, K. S., & Cek, K. (2024). Influence of blockchain and artificial intelligence on audit quality: Evidence from Turkey. *Heliyon*, *10*(9), e30166. https://doi.org/10.1016/j.heliyon.2024.e30166

Rozario, A. M., & Thomas, C. (2019). Reengineering the audit with blockchain and smart contracts. *Journal of Emerging Technologies in Accounting*, *16*(1), 21–35. https://doi.org/10.2308/jeta-52432

Rozario, A. M., & Vasarhelyi, M. A. (2018). Auditing with smart contracts. *The International Journal of Digital Accounting Research*, *18*(1), 1–27. https://doi.org/10.4192/1577-8517-v18_1

Schmitz, J., & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: A research agenda. *Australian Accounting Review*, *29*(2), 331–342. https://doi.org/10.1111/auar.12278

Secinaro, S., Calandra, D., Biancone, P., & Busso, D. (2021). Blockchain in the accounting, auditing and accountability fields: A bibliometric and coding analysis. *Accounting, Auditing & Accountability Journal*, *35*(9), 1–28. https://doi.org/10.1108/AAAJ-09-2020-4872

Sheldon, M. D. (2021). Auditing the blockchain oracle problem. *Journal of Information Systems*, *35*(1), 121–133. https://doi.org/10.2308/ISYS-19-049

Sheldon, M. D. (2022). Auditing with blockchain technology. *Journal of Emerging Technologies in Accounting*, *19*(1), 129–141. https://doi.org/10.2308/JETA-2021-032

Silva, T., Teixeira, V., Martins, J., & Santos, V. (2022). Blockchain implications for auditing: A systematic literature review and bibliometric analysis. *The International Journal of Digital Accounting Research*, *22*, 175–215. https://www.researchgate.net/publication/364566751

Tušek, B., Ježovita, A., & Halar, P. (2021). The importance and differences of analytical procedures' application for auditing blockchain technology between external and internal auditors in Croatia. *Economic Research-Ekonomska Istraživanja*, *34*(1), 1385–1408. https://doi.org/10.1080/1331677X.2020.1828129

Vacca, A., Di Sorbo, A., Visaggio, C. A., & Canfora, G. (2021). A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. *Journal of Systems and Software*, *174*, 110891. https://doi.org/10.1016/j.jss.2020.110891

Ziemba, E. W., Renik, K., Maruszewska, E. W., & Mullins, R. (2025). Blockchain adoption in auditing: A systematic literature review. *Central European Management Journal*. https://doi.org/10.1108/CEMJ-06-2024-0196