

Prosperia: Journal of Economic Development, Accounting, and Global Markets
Vol 1 No 4 November 2026, Hal 79-89
ISSN: 3125-117x (Print) ISSN: 3125-1181 (Electronic)
Open Access: https://sovereignresearch.org/prosperia

AI-Blockchain Integration in Auditing: Accountability Trade-offs and the Compliance Trilemma

Patrick Boamah[1]
[1] University of Skills Training and Entrepreneurial Development, Ghana
email: boamahpatrick36@gmail.com[1]

Article Info :
Received:
26-08-2026
Revised:
26-10-2026
Accepted:
05-11-2026

Abstract

This paper examines how the combined use of artificial intelligence (AI) and blockchain may change accountability in auditing, including professional judgement, liability allocation and the profession's jurisdiction. An interpretive thematic synthesis of 270 academic, professional and regulatory documents (2015–2025) was conducted using Braun and Clarke's reflexive thematic analysis. The synthesis identifies three mechanisms: Intelligent Immutability, Automated Assurance and Verifiable Explainability. Their interaction suggests a Compliance Trilemma, offered as a conceptual proposition: transparency, data privacy and automation cannot all be maximised in the same system when personal data are stored on an unredactable ledger and automated actions require full data access in real time. Design choices such as permissioned ledgers and off-chain storage can ease these tensions but shift costs elsewhere. The framework has not yet been tested empirically. It offers researchers propositions for testing and helps practitioners make design trade-offs and the allocation of responsibility explicit.

Keywords: *Accountability, AI–Blockchain Integration, Audit Assurance, Compliance Trilemma, Professional Jurisdiction*

©2026 Authors.. This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.
(https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUCTION

Auditing rests on negotiated arrangements of expertise, trust and accountability among preparers, auditors, regulators and the public. The combined use of artificial intelligence (AI) and blockchain is beginning to unsettle these arrangements by changing the evidence auditors rely on, where judgement is exercised and who answers for outcomes (Power, 2008; Robson & Bottausci, 2018; Jeacle & Carter, 2022). Accounting research has studied each technology in depth. Work on AI shows audit practice moving from sampling and rule-based testing toward continuous, data-driven and predictive assurance (Kokina & Davenport, 2017; Issa et al., 2016; Moffitt et al., 2018). Work on blockchain examines record integrity, triple-entry bookkeeping, real-time reporting and the automation of compliance through smart contracts (Coyne & McMickle, 2017; Dai & Vasarhelyi, 2017; Alles & Gray, 2020).

A smaller body of work combines the two. It proposes architectures for AI-supported risk management on distributed ledgers (Rahman et al., 2024) and maps blockchain applications in accounting and auditing (Georgiou et al., 2024). These studies are mainly concerned with design and performance: how the technologies can be joined and what efficiency or detection gains follow. Accountability enters, if at all, as a technical property of the system. Three questions therefore remain open: how integration redistributes judgement and liability among auditors, system operators and technology vendors; why integrated systems meet resistance from privacy law and regulators; and which consequences belong to integration itself.

The last question needs care, because each technology already raises accountability problems on its own. AI brings opacity and the risk that scepticism gives way to reliance on model outputs (Moll & Yigitbasioglu, 2019). Blockchain brings conflict between permanent records and erasure rights, and the prospect of controls that run without auditors (Dai & Vasarhelyi, 2017). Integration adds problems of a different kind. A probabilistic AI judgement can trigger an automatic and hard-to-reverse contract action. Logs of AI decisions become permanent. Model outputs may acquire the authority of tamper-evident records, although the ledger cannot vouch for the accuracy of what was entered (Alles & Gray, 2020). These integration-specific effects are the focus of this study.

The study asks how AI–blockchain integration changes the allocation of accountability in auditing and what tensions this produces. Its objectives are to identify the mechanisms through which integration, as distinct from either technology alone, alters audit evidence, judgement and liability; to develop a proposition about trade-offs among transparency, data privacy and automation and the conditions under which they bind; and to consider implications for professional jurisdiction and the allocation of responsibility among auditors, system operators and vendors.

To meet these objectives, the study conducts an interpretive thematic synthesis of 270 academic, professional and regulatory documents published between 2015 and 2025. The synthesis identifies three mechanisms, Intelligent Immutability, Automated Assurance and Verifiable Explainability, and proposes the Compliance Trilemma: the argument that transparency, data privacy and automation cannot all be maximised in the same system under specified conditions. The Trilemma is offered as a conceptual proposition for empirical testing.

The contribution is theoretical. Drawing on Abbott's (1988) theory of professional jurisdiction and on accounting research on the limits of accountability (Roberts, 2009; Messner, 2009; McKernan, 2012), the study moves the analysis of audit technology from questions of efficiency to questions of who is answerable, to whom, and at what cost. For practitioners and standard-setters, the framework offers a way to make design trade-offs explicit before adoption.

The audit profession rests on a long-standing settlement. Registered auditors hold exclusive rights to verify financial statements and, in return, accept accountability to clients, regulators, investors and the public (Abbott, 1988; Power, 2008; Robson & Bottausci, 2018). AI and blockchain are beginning to unsettle this settlement by changing how accounting information is produced, checked and held to account (Jeacle & Carter, 2022; Quattrone, 2016). Accounting research has examined the two technologies mainly in separate streams. Studies that combine them exist but focus chiefly on system design and performance, leaving their accountability consequences largely unexplored. This section reviews both streams, considers the work that joins them, and sets out the study's theoretical framing.

Research on AI in auditing has moved through broadly three phases. Early work was optimistic, presenting machine learning and advanced analytics as the route to continuous auditing (Vasarhelyi et al., 2015; Issa et al., 2016; Krahel & Titera, 2015). Moving from periodic sampling to monitoring of whole populations, it was argued, would free auditors from routine tasks and let them concentrate on judgement-intensive work (Kokina & Davenport, 2017; Moffitt et al., 2018). Later studies offered a more mixed view. AI reduces the manual burden of journal-entry testing and reconciliation, but it also brings probabilistic logic into risk assessment and anomaly detection, areas previously governed by professional judgement (Appelbaum et al., 2017; Sun & Vasarhelyi, 2018).

More critical work raises the risk of de-skilling. When algorithms decide what counts as unusual, scepticism may narrow to accepting outputs the auditor cannot inspect (Moll & Yigitbasioglu, 2019; Pérez-Calderón et al., 2025). Professional bodies now call for AI used in finance and audit to be explainable and well governed (ICAEW, 2025; IFAC, 2024), yet many high-performing models remain difficult to interpret. This tension between analytical power and accountability leaves open whether AI strengthens or weakens auditing's public-interest role. Blockchain research in accounting followed a similar path. Early studies welcomed blockchain for tamper-evident records, fewer reconciliations and the prospect of triple-entry bookkeeping (Coyne & McMickle, 2017; Dai & Vasarhelyi, 2017; Wang & Kogan, 2018). Smart contracts drew particular interest because they appeared able to automate compliance and reduce reliance on manual verification (Dai & Vasarhelyi, 2017).

Subsequent work identified three limits. First, most commercial applications use permissioned ledgers, which restore a degree of central control and require confidentiality to be designed in (Wang & Kogan, 2018). Second, permanent records sit uneasily with erasure rights under the GDPR (European Union, 2016, Article 17), although the severity of the conflict depends on what is stored on-chain. Third, ledger integrity does not guarantee that recorded transactions are accurate or legitimate, so the demand for independent assurance persists (Alles & Gray, 2020; Coyne & McMickle, 2017). New assets and records on blockchains also create audit difficulties of their own (Vincent & Wilkins, 2020). Whether smart contracts ultimately displace or extend the auditor's role remains an open question.

The two literatures still meet only occasionally. Studies of AI in auditing repeatedly cite data quality, provenance and bias as limitations but rarely consider ledger-based records as part of the answer (Cao et al., 2015; Sun & Vasarhelyi, 2018; Yaseen & Al-Amarneh, 2025). Blockchain studies, in turn, focus on immutability and automation and give less attention to how machine learning might operate

on ledger data (Georgiou et al., 2024). Work that joins the two, such as proposed AI–blockchain architectures for risk management (Rahman et al., 2024), concentrates on technical design and reported performance.

This gap matters for accounting research for three reasons. First, audit firms present AI and blockchain tools side by side in their technology strategies (PwC, 2017; EY, 2024), so practice may be moving faster than research toward combined systems. Second, accounting scholars have long argued that technological change in assurance should be studied as a combination of people, tools and rules rather than tool by tool (Robson & Bottausci, 2018; Quattrone, 2016; Justesen & Mouritsen, 2011). Third, studying the technologies separately leaves unexamined how transparency, privacy, automation and professional judgement may come into conflict once the technologies are combined.

The study draws on Abbott's (1988) theory of professional jurisdiction and Power's (2008) audit-society thesis. From this perspective, AI–blockchain integration can be read as a contest over who, or what, performs legitimate assurance work. Three mechanisms, developed in detail in the findings, frame the analysis: Intelligent Immutability: AI analytics run on tamper-evident records. It strengthens the integrity of evidence after recording, while raising questions about the accuracy of what was recorded and whose models define anomalies. Automated Assurance: AI risk scores trigger smart-contract actions. It shortens the interval between transaction, detection and response, while spreading liability across deployers, vendors, developers and auditors. Verifiable Explainability: ledgers record which model, data and version produced an AI decision. It improves traceability, while creating possible conflicts with data-protection law.

Taken together, these mechanisms point toward what this study proposes as the Compliance Trilemma: under specified conditions, transparency, data privacy and automation cannot all be maximised in the same system. Because each design choice favours some actors and accountability relations over others, the trade-offs are organisational and political as well as technical (Roberts, 2009; Messner, 2009; McKernan, 2012). The framework thus responds to calls for sociologically informed studies of audit technology (Jeacle & Carter, 2022; Moll & Yigitbasioglu, 2019).

RESEARCH METHODS

This study uses an interpretive thematic synthesis to develop theory on the accountability implications of AI–blockchain integration in auditing. The research question concerns how integration changes the allocation of judgement, liability and visibility in assurance, rather than whether it improves efficiency. Such a question calls for interpretation across academic, professional and regulatory texts more than for the pooled effect sizes a meta-analysis would provide. Thematic synthesis suits this aim because it combines systematic searching and documented screening with interpretive coding capable of producing new constructs (Thomas & Harden, 2008; Parker & Northcott, 2016). Here it yields three mechanisms and a conceptual proposition, the Compliance Trilemma, intended for later empirical testing.

Data Sources and Selection Strategy

The corpus drew on three bodies of text, so that academic claims could be read against the professional and regulatory discourses that shape practice.

Academic literature. Scopus and Web of Science were searched in March 2025, with an update in November 2025, and Google Scholar was used to check for missed items. Search strings combined audit terms ("audit" OR "assurance" OR "accounting profession" OR "professional jurisdiction" OR "audit accountability") with technology terms ("artificial intelligence" OR "machine learning" OR "blockchain" OR "distributed ledger" OR "smart contract"), limited to English-language work published 2015–2025. The core set was restricted to journals rated 3, 4 or 4* in the Academic Journal Guide (ABS). This filter served as a quality threshold for theoretical claims about accountability and the profession, the study's main concern. Because it risked missing technical work on integrated architectures, which appears mostly in information-systems and computer-science outlets, 15 peer-reviewed papers from outside the ranking were admitted where they described AI–blockchain designs absent from ranked accounting journals. These 15 papers are included in the 200 academic sources and informed the description of mechanisms, but not claims about professional or organisational outcomes.

Professional and grey literature. Forty-two documents from audit firms, technology vendors and professional bodies (ICAEW, IFAC, FRC, PCAOB, IAASB), published 2017–2025, were collected

from the issuers' websites. They show how practice is being framed before academic study catches up (Power, 2015).

Regulatory documents. Twenty-eight texts from the IAASB, PCAOB, FRC, ESMA and the European Commission, issued 2021–2025, covered audit technology, AI and distributed ledgers. Each was classified as binding (legislation, adopted standards) or advisory (consultations, guidance, market scans), and the analysis kept this distinction.

Credibility appraisal. Non-academic documents were appraised on the authority of the issuer, the transparency of any data or method reported, and the issuer's commercial interest in the technology. Performance figures in vendor or firm material were recorded as claims and were not treated as evidence of outcomes unless independently documented.

Screening. Table 1 summarises the selection trail. After duplicates were removed, titles and abstracts were screened against a single inclusion criterion: substantive discussion of AI, blockchain or both in an auditing, assurance or financial-reporting context. Remaining records were assessed in full text. The final corpus contained 270 documents, concentrated in 2021–2025.

Table 1. Selection Trail

Stage	Academic	Grey literature	Regulatory	Total
Records identified	845	115	64	1,024
After duplicates removed	620	85	45	750
Excluded at title/abstract	310	30	12	352
Full texts assessed	310	55	33	398
Excluded at full text	110	13	5	128
Final corpus	200	42	28	270

Analytical Procedure

Analysis followed Braun and Clarke's (2006, 2021) reflexive thematic analysis and was carried out entirely by the author. In this approach the researcher's interpretation is the analytic instrument, so agreement between coders is neither expected nor treated as a marker of quality (Braun & Clarke, 2021). Rigour rests instead on a documented trail of codes, memos and decisions. NVivo 14 was used to store the corpus, apply codes and retrieve coded extracts. The software did not generate codes or themes; all coding and theme construction were done manually.

Familiarisation involved repeated reading, with memos on shifts in accountability, jurisdictional claims and expressed tensions. Coding proceeded line by line, beginning with deductive codes drawn from Abbott (1988), Power (2008) and Roberts (2009), including "jurisdictional threat" and "liability displacement", and adding inductive codes such as "immutability–privacy collision" and "explainability theatre". The final codebook contained 48 codes.

Theme development grouped codes into candidate themes through constant comparison, with decisions recorded in memos. The candidate themes were reviewed against the full dataset and contrasting cases, including public and permissioned ledgers. Definition and naming retained the three mechanisms and the Compliance Trilemma as the most coherent structure. Writing up combined the coded extracts with theoretical interpretation.

Saturation was assessed by coding the corpus in batches of about 30 documents. It was judged reached when the final batch added no new codes and left the theme structure unchanged; the last new code appeared at document 238 of 270.

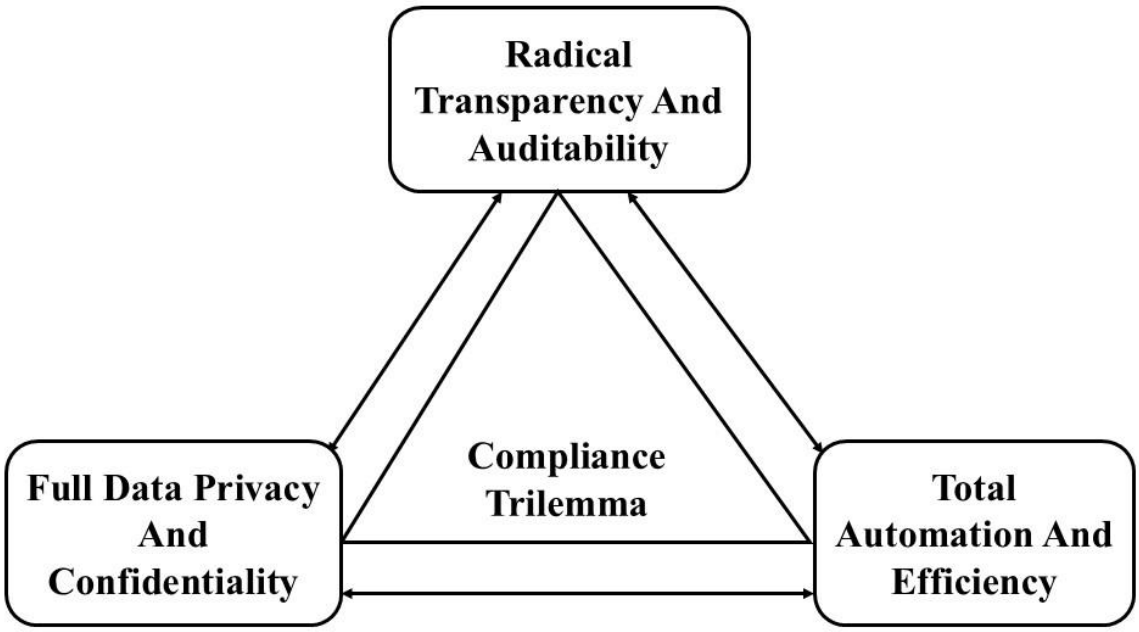


Figure 1. AI–Blockchain Integration and the Emergent Compliance Trilemma: A Socio-Technical Accountability Framework
Source: Developed from the literature for this study.

Quality was judged by transparency of process, theoretical coherence and plausibility of interpretation (Ahrens & Chapman, 2006; Lukka & Modell, 2010). Reflexive memos recorded how the author's background in audit regulation and technology governance shaped, and was challenged by, the analysis.

After the initial themes were drafted, the framework was discussed with three practitioners: two audit-innovation partners from Big Four firms and one technical adviser to the IAASB. The sessions were individual online meetings of about 60 minutes held in April 2025. Participants received a summary of the mechanisms and the Trilemma and were asked whether they recognised the tensions and where the framework failed to fit their experience. Their comments led to the explicit treatment of ledger type (permissioned or public) as a moderating factor within the Automated Assurance mechanism, and to the renaming of the third mechanism to better capture cryptographic audit trails. These sessions tested plausibility and do not constitute empirical validation.

The corpus is limited to published and publicly released material. Proprietary systems, failed pilots and informal regulatory arrangements are largely absent, which may tilt the corpus toward positive accounts. The ABS restriction may have excluded relevant technical work, though the supplementary set partly offsets this. Developments after late 2025 are not covered. Finally, the framework is derived from texts, not from observation of practice, and its propositions require empirical testing.

RESULTS AND DISCUSSION

The synthesis identified three mechanisms through which AI–blockchain integration reshapes assurance: Intelligent Immutability, Automated Assurance and Verifiable Explainability. They are presented as analytical constructs drawn from the corpus, not as measured organisational outcomes. Much of the evidence on integrated systems comes from pilots, vendor material and conceptual papers, so each subsection states what the sources can and cannot show. the cross-mechanism analysis then

examines how the mechanisms interact and proposes the Compliance Trilemma as a proposition for empirical testing.

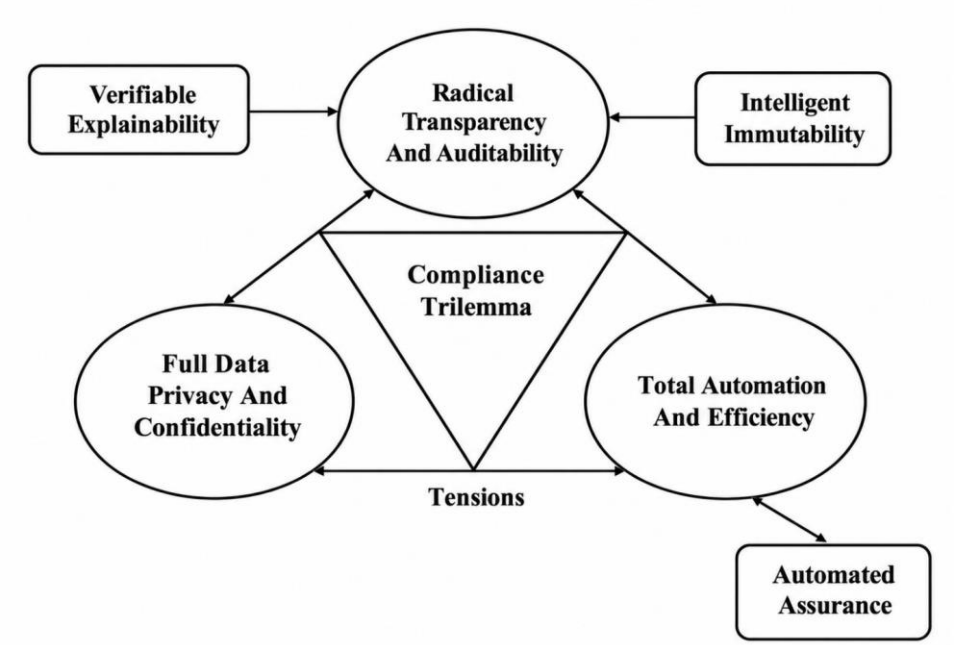


Figure 2. The Compliance Trilemma and Its Relationship to the Three Emergent Socio-Technical Mechanisms
Source: Derived from the interpretive thematic synthesis.

Figure 2 makes the relationships among the three socio-technical mechanisms and the competing goals explicit. Intelligent Immutability and Verifiable Explainability relate to auditability and transparency, whereas Automated Assurance foregrounds the conditions under which rapid control actions may intensify tensions with confidentiality and data privacy.

Intelligent Immutability

Intelligent Immutability refers to AI analytics run on records held in a tamper-evident ledger. The corpus increasingly treats blockchain as a data layer for analytics rather than a stand-alone audit tool. The attraction is provenance: AI procedures depend on reliable inputs, and a ledger shows when a record was created and whether it has since changed (Dai & Vasarhelyi, 2017). In principle, this allows anomaly detection across full transaction populations instead of samples. Documented examples remain scarce, however. Most sources describe prototypes (e.g. Rahman et al., 2024), with gains reported only in controlled or vendor-defined settings.

Two limits qualify the mechanism. First, a ledger shows that a record has not changed since it was written, not that it was accurate or authorised when entered. Alles and Gray (2020) call this the "first mile problem": errors and fraud at the point of entry are preserved as faithfully as legitimate transactions (see also Coyne & McMickle, 2017). Auditors must still test entry controls and the link between entries and the events they record. Second, record integrity makes training data easier to trace but does not remove selection bias, inaccurate inputs or discriminatory patterns in a model. Since flawed records stay permanently in the data set, such problems may become harder to correct.

If audit teams treat ledger-based AI outputs as settled fact, the room for professional scepticism narrows (Moll & Yigitbasioglu, 2019). Intelligent Immutability thus strengthens the integrity of evidence after recording, while its accuracy still depends on human judgement and controls outside the chain.

Automated Assurance

Automated Assurance describes arrangements in which smart contracts carry out compliance actions and AI models decide when to trigger them. A smart contract alone executes fixed rules; an added model lets the trigger depend on a contextual risk score. In designs described in the corpus, a

model flags unusual ledger activity and calls a contract that holds a payment or raises an alert (Rahman et al., 2024), extending continuous assurance (Dai & Vasarhelyi, 2017) into automatic response.

The evidence is thin. The corpus contains no independently documented case of an AI-triggered smart contract in live audit or compliance use. Audit firms' AI announcements (e.g. KPMG, 2024) concern analytics, not blockchain enforcement, and vendor efficiency claims cannot be generalised. It remains an emerging design pattern, and ledger type moderates it: on a permissioned ledger an operator can pause or reverse a contract's action, whereas on a public ledger reversal is much harder.

With AI alone, a person usually acts on the output; a smart contract alone applies a fixed rule open to inspection. Combined, a probabilistic judgement leads directly to an action that is hard to reverse. As Lessig (2000) argues, code works as regulation, set by system designers often outside the audit relationship. If such a contract wrongly blocks legitimate funds, responsibility could rest with the deployer, the model vendor, the developers or the auditor, and the documents reviewed offer no settled guidance. The auditor's role may shift from judging transactions to assessing the system that judges them (Abbott, 1988).

Verifiable Explainability

Verifiable Explainability refers to the use of a ledger to keep a tamper-evident record of how an AI system reached its outputs: which model version ran, on which data, and when. Its appeal lies in the gap between the opacity of machine learning and the demand for traceable evidence in assurance. A permanent log does not explain a model's reasoning, but it lets an auditor confirm afterwards which model and inputs produced a given decision. In the corpus this appears mainly as a proposal in conceptual and professional sources (e.g. Rahman et al., 2024) rather than as documented practice.

The regulatory position is more limited than some sources suggest. GDPR Article 22 restricts decisions based solely on automated processing that have legal or similarly significant effects; it does not create a general right to explanation, and the scope of any such right remains contested (Wachter et al., 2017). The EU AI Act (European Union, 2024) is binding law and requires record-keeping for high-risk systems, whereas professional guidance on AI audit trails is advisory. Whether permanent logging conflicts with erasure rights depends on design. Storing hashes on-chain and personal data off-chain eases the conflict, while writing personal data directly to an immutable ledger sharpens it.

The analysis also produced an inductive code labelled "explainability theatre": logs that look complete but leave bias and model weaknesses unexamined. Where verification centres on logs, the auditor's work may move from interpreting business context toward checking records of code.

Cross-Mechanism Insights: The Compliance Trilemma

Read together, the three mechanisms pull in different directions. Intelligent Immutability and Verifiable Explainability increase transparency by producing detailed, permanent audit trails. Automated Assurance increases efficiency by placing controls inside the transaction flow. The cross-thematic analysis suggests that pushing both goals together brings them into conflict with a third, data privacy. This study names that tension the Compliance Trilemma and offers it as a conceptual proposition, not a demonstrated finding.

The proposition is that transparency, privacy and automation cannot all be maximised in the same system. Permanent, detailed logs sit uneasily with erasure and data-minimisation duties under the GDPR. Privacy safeguards, in turn, add review steps, access limits and pauses that slow automated processing. Design choices can ease these tensions. Permissioned ledgers restrict who sees records, off-chain storage keeps personal data off the immutable layer, and zero-knowledge proofs allow a fact to be verified without revealing the data behind it. Each choice, however, has a cost: control becomes more centralised, systems grow more complex, or verification depends on trust in whoever holds the off-chain data.

The trade-offs are therefore expected to bind most tightly under particular conditions: when personal data are written directly to the ledger, when the ledger is public and cannot be redacted, and when automated actions require full data access in real time. Outside these conditions they may be manageable. Where they do bind, organisations must choose which goal to favour, and that choice decides whose accountability claims prevail, such as regulators' over data subjects', or system designers' over auditors'. The trade-offs are thus organisational and jurisdictional as well as technical, a claim that requires empirical testing.

Much of the accounting information systems and fintech literature treats AI and blockchain as complementary technologies whose combination will raise efficiency, fraud detection and compliance. The findings point to a more mixed picture. The three mechanisms can strengthen particular features of assurance, but their interaction also brings existing accountability tensions into sharper view and, under certain conditions, forces choices among competing goals.

Reassembling Accountability Relations

In some respects, the mechanisms address long-standing aims of the audit society (Power, 2008). Intelligent Immutability speaks to concerns over data provenance in AI-driven auditing (Moffitt et al., 2018), although, as the Intelligent Immutability analysis showed, ledger integrity does not establish that recorded data are accurate (Alles & Gray, 2020). Automated Assurance extends the ambition of continuous auditing (Vasarhelyi et al., 2015; Dai & Vasarhelyi, 2017). Verifiable Explainability offers a partial response to the opacity of algorithmic decisions, a concern raised by regulators and critical scholars alike (Jeacle & Carter, 2022).

Greater visibility has costs of its own. Accounting technologies carry the interests of those who design them and can reorder power relations (Robson & Bottausci, 2018; Quattrone, 2016). The mechanisms described here may move judgement from auditors to combined human and technical systems, spread liability across deployers, vendors and developers, and shorten the interval between transaction and control. Read through Abbott's (1988) theory of professional jurisdiction, this amounts to a potential challenge to the profession's claim to exclusive expertise in verification. How far that challenge develops in practice is an empirical question that the present analysis cannot settle.

The Compliance Trilemma as a Conceptual Proposition

The main contribution of this study is the Compliance Trilemma as a conceptual proposition. Earlier work frames technology trade-offs in pairs, such as efficiency against scepticism or automation against judgement. The Trilemma adds a third term, data privacy, and links all three to identifiable design choices. the cross-mechanism analysis argued that the trade-offs bind most tightly when personal data sit on the ledger itself, when the ledger is public and cannot be redacted, and when automated actions need full data access in real time. Permissioned ledgers, off-chain storage and zero-knowledge proofs can ease the tensions, but they move the cost toward centralised control, added complexity or reliance on an off-chain data holder.

Each design choice therefore affects stakeholders differently. Public or permissioned ledgers, on-chain or off-chain logging, and interpretable or high-performance models each favour some parties, for example regulators or senior management, over others, such as data subjects or smaller audit firms. This places the Trilemma within the critical tradition that treats accounting technologies as political (Arnaboldi et al., 2017; Troshani et al., 2019). It also connects with Power's (2008) argument that the audit society produces new risks as it governs old ones. Systems designed to make assurance more transparent and automated may weaken forms of accountability that depend on privacy, deliberation and professional judgement. Whether this occurs in practice, and under which conditions, requires empirical study.

Theoretical Implications

Three theoretical implications follow. First, agency-based accounts present new technologies as monitoring devices that reduce information asymmetry between principals and agents (Jensen & Meckling, 1976). The analysis suggests that asymmetry may change form instead of disappearing, as discretion moves into systems that are themselves hard to inspect or hold responsible (Roberts, 2009; Messner, 2009). Second, the framework adds to complementarity theory (Milgrom & Roberts, 1995) by specifying mechanisms through which AI and blockchain reinforce each other and by proposing that, beyond certain points, those complementarities produce tensions of their own. Third, the Trilemma may serve as a mid-range construct for studying other data-intensive assurance settings, such as sustainability reporting, tax transparency and ESG data chains, where similar tensions are likely to arise.

Professional Jurisdiction and the Public Interest

If assurance increasingly relies on automated systems, the profession's traditional basis for legitimacy, accepting liability in return for exclusive jurisdiction, comes under pressure (Abbott, 1988).

Standard-setters may need to decide whether to strengthen human oversight, at some cost to automation, or to redefine auditors as assurers of the systems that perform controls.

These choices sit within a mixed regulatory landscape. The GDPR and the EU AI Act are binding law. Auditing standards issued by the IAASB and PCAOB bind auditors within their jurisdictions, whereas consultation papers, market scans and professional guidance are advisory. Much of the material on AI–blockchain assurance in the corpus belongs to the advisory category. Responsibility among auditors, system operators and technology vendors therefore remains largely unsettled, and the Trilemma offers a way to make the trade-offs behind that allocation explicit.

CONCLUSION

This study has examined how the combined use of AI and blockchain may change accountability in auditing. Through an interpretive thematic synthesis of 270 documents, it identified three mechanisms, Intelligent Immutability, Automated Assurance and Verifiable Explainability, and proposed the Compliance Trilemma: under specified conditions, transparency, data privacy and automation cannot all be maximised in the same system. The contribution is conceptual. The mechanisms and the Trilemma are derived from published texts and practitioner discussion, not from observation of organisations, and they should be read as propositions for testing. Their value lies in showing that design choices for integrated systems also allocate accountability, and in specifying when the trade-offs are likely to bind: when personal data are written to the ledger, when the ledger is public and cannot be redacted, and when automated actions require full data access in real time.

REFERENCES

Abbott, A. (1988). *The system of professions: An essay on the division of expert labor*. University of Chicago Press. https://doi.org/10.7208/chicago/9780226189666.001.0001

Ahrens, T., & Chapman, C. S. (2006). Doing qualitative field research in management accounting: Positioning data to contribute to theory. *Accounting, Organizations and Society*, 31(8), 819–841. https://doi.org/10.1016/j.aos.2006.03.007

Alles, M., & Gray, G. L. (2020). "The first mile problem": Deriving an endogenous demand for auditing in blockchain-based business processes. *International Journal of Accounting Information Systems*, 38, 100465. https://doi.org/10.1016/j.accinf.2020.100465

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory*, 36(4), 1–27. https://doi.org/10.2308/ajpt-51684

Arnaboldi, M., Busco, C., & Cuganesan, S. (2017). Accounting, accountability, social media and big data: Revolution or hype? *Accounting, Auditing & Accountability Journal*, 30(4), 762–776. https://doi.org/10.1108/aaaj-03-2017-2880

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE.

Cao, M., Chychyla, R., & Stewart, T. (2015). Big data analytics in financial statement audits. *Accounting Horizons*, 29(2), 423–429. https://doi.org/10.2308/acch-51068

Coyne, J. G., & McMickle, P. L. (2017). Can blockchains serve an accounting purpose? *Journal of Emerging Technologies in Accounting*, 14(2), 101–111. https://doi.org/10.2308/jeta-51910

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

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L, 12 July 2024.

EY. (2024). EY Blockchain Analyzer: Reconciler [Solution brief]. https://blockchain.ey.com/uploads/EY%20Blockchain%20Analyzer_Solution_Brief_2024.pdf

Georgiou, I., Sapuric, S., Lois, P., & Thrassou, A. (2024). Blockchain for accounting and auditing—Accounting and auditing for cryptocurrencies: A systematic literature review and future research

directions. *Journal of Risk and Financial Management*, 17(7), 276. https://doi.org/10.3390/jrfm17070276

Institute of Chartered Accountants in England and Wales (ICAEW). (2025). Accountants are embracing AI and securing their future. https://www.icaew.com/insights/viewpoints-on-the-news/2025/mar-2025/accountants-are-embracing-ai-and-securing-their-future

International Federation of Accountants (IFAC). (2024). Harnessing innovation: Exploring the responsible use of AI in finance and accounting. https://www.ifac.org/knowledge-gateway/discussion/harnessing-innovation-exploring-responsible-use-ai-finance-and-accounting

Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. *Journal of Emerging Technologies in Accounting*, 13(2), 1–20. https://doi.org/10.2308/jeta-10511

Jeacle, I., & Carter, C. (2022). Audit society goes viral: The rise of the online auditor. *Qualitative Research in Accounting & Management*, 19(2), 231–240. https://doi.org/10.1108/qram-10-2021-0185

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. https://doi.org/10.1016/0304-405x(76)90026-x

Justesen, L., & Mouritsen, J. (2011). Effects of actor-network theory in accounting research. *Accounting, Auditing & Accountability Journal*, 24(2), 161–193. https://doi.org/10.1108/09513571111100672

Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. *Journal of Emerging Technologies in Accounting*, 14(1), 115–122. https://doi.org/10.2308/jeta-51730

KPMG. (2024). KPMG announces AI integration into global smart audit platform, KPMG Clara. https://kpmg.com/us/en/media/news/kpmg-ai-integration-clara-2024.html

Krahel, J. P., & Titera, W. R. (2015). Consequences of big data and formalization on accounting and auditing standards. *Accounting Horizons*, 29(2), 409–422. https://doi.org/10.2308/acch-51065

Lessig, L. (2000). *Code: And other laws of cyberspace*. Basic Books.

Lukka, K., & Modell, S. (2010). Validation in interpretive management accounting research. *Accounting, Organizations and Society*, 35(4), 462–477. https://doi.org/10.1016/j.aos.2009.10.004

McKernan, J. F. (2012). Accountability as aporia, testimony, and gift. *Critical Perspectives on Accounting*, 23(3), 258–278. https://doi.org/10.1016/j.cpa.2011.12.009

Messner, M. (2009). The limits of accountability. *Accounting, Organizations and Society*, 34(8), 918–938. https://doi.org/10.1016/j.aos.2009.07.003

Milgrom, P., & Roberts, J. (1995). Complementarities and fit: Strategy, structure, and organizational change in manufacturing. *Journal of Accounting and Economics*, 19(2–3), 179–208. https://doi.org/10.1016/0165-4101(94)00382-f

Moffitt, K. C., Rozario, A. M., & Vasarhelyi, M. A. (2018). Robotic process automation for auditing. *Journal of Emerging Technologies in Accounting*, 15(1), 1–10. https://doi.org/10.2308/jeta-10589

Moll, J., & Yigitbasioglu, O. (2019). The role of internet-related technologies in shaping the work of accountants: New directions for accounting research. *The British Accounting Review*, 51(6), 100833. https://doi.org/10.1016/j.bar.2019.04.002

Parker, L. D., & Northcott, D. (2016). Qualitative generalising in accounting research: Concepts and strategies. *Accounting, Auditing & Accountability Journal*, 29(6), 1100–1131. https://doi.org/10.1108/aaaj-04-2015-2026

Pérez-Calderón, E., Alrahamneh, S. A., & Milanés Montero, P. (2025). Impact of artificial intelligence on auditing: An evaluation from the profession in Jordan. Discover Sustainability, 6, Article 251. https://doi.org/10.1007/s43621-025-01058-3

Power, M. (2008). Research evaluation in the audit society. In *VS Verlag für Sozialwissenschaften eBooks* (pp. 15–24). https://doi.org/10.1007/978-3-531-90863-2_2

Power, M. (2015). How accounting begins: Object formation and the accretion of infrastructure. *Accounting, Organizations and Society*, 47, 43–55. https://doi.org/10.1016/j.aos.2015.10.005

PricewaterhouseCoopers (PwC). (2017). Transforming the audit through technology, AI, and human insight. https://www.pwc.com/us/en/about-us/newsroom/press-releases/reimagining-audit-with-ai-technology.html

Quattrone, P. (2016). Management accounting goes digital: Will the move make it wiser? *Management Accounting Research*, 31, 118–122. https://doi.org/10.1016/j.mar.2016.01.003

Rahman, M. M., Pokharel, B. P., Sayeed, S. A., Bhowmik, S. K., Kshetri, N., & Eashrak, N. (2024). riskAIchain: AI-driven IT infrastructure—Blockchain-backed approach for enhanced risk management. Risks, 12(12), 206. https://doi.org/10.3390/risks12120206

Roberts, J. (2009). No one is perfect: The limits of transparency and an ethic for 'intelligent' accountability. *Accounting, Organizations and Society*, 34(8), 957–970. https://doi.org/10.1016/j.aos.2009.04.005

Robson, K., & Bottausci, C. (2018). The sociology of translation and accounting inscriptions: Reflections on Latour and accounting research. *Critical Perspectives on Accounting*, 54, 60–75. https://doi.org/10.1016/j.cpa.2017.11.003

Sun, T., & Vasarhelyi, M. A. (2018). Embracing textual data analytics in auditing with deep learning. *The International Journal of Digital Accounting Research*, 18, 49–67. https://doi.org/10.4192/1577-8517-v18_3

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, 8, 45. https://doi.org/10.1186/1471-2288-8-45

Troshani, I., Locke, J., & Rowbottom, N. (2019). Transformation of accounting through digital standardisation: Tracing the construction of the IFRS Taxonomy. *Accounting, Auditing & Accountability Journal*, 32(1), 133–162. https://doi.org/10.1108/aaaj-11-2016-2794

Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big data in accounting: An overview. *Accounting Horizons*, 29(2), 381–396. https://doi.org/10.2308/acch-51071

Vincent, N. E., & Wilkins, A. M. (2020). Challenges when auditing cryptocurrencies. *Current Issues in Auditing*, 14(1), A46–A58. https://doi.org/10.2308/ciia-52675

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving blockchain-based transaction processing systems. *International Journal of Accounting Information Systems*, 30, 1–18. https://doi.org/10.1016/j.accinf.2018.06.001

Yaseen, H., & Al-Amarneh, A. (2025). Adoption of artificial intelligence-driven fraud detection in banking: The role of trust, transparency, and fairness perception in financial institutions in the United Arab Emirates and Qatar. *Journal of Risk and Financial Management*, 18(4), 217. https://doi.org/10.3390/jrfm18040217