International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 8.141
Peer Reviewed Bi-Monthly
Vol. 7 No. 48 July – Aug - 2026

Transforming Financial Assurance: A Conceptual Framework for Integrating Artificial Intelligence and Blockchain in Auditing Processes

Rajesh Gidwani[1] & Mr. Jigar Aggarwal[2]

[1] *Research Scholar*

[2]*Research Guide & Associate Professor, J.G. University, Gujarat University*

Corresponding Author – Rajesh Gidwani

DOI - 10.5281/zenodo.23602004

Abstract:

The accounting and auditing professions are undergoing a profound technological transformation driven by the convergence of Artificial Intelligence (AI) and blockchain technology. AI provides advanced capabilities for pattern recognition, anomaly detection, predictive analytics, natural language processing, and automated review of large volumes of financial and non-financial information. Blockchain, in contrast, provides a distributed and cryptographically secured record of transactions that can strengthen traceability, data integrity, and transparency. This conceptual paper examines how the combined application of AI and blockchain can transform accounting and auditing from predominantly periodic, sample-based activities toward continuous and risk-focused assurance. Drawing on the existing conceptual and professional literature, the paper develops a four-layer Continuous Assurance Architecture comprising data ingestion and transaction generation, blockchain-based verification and immutable storage, AI-enabled cognitive analysis and anomaly detection, and continuous reporting and decision support. The framework explains how blockchain can provide a more reliable transaction history while AI can interpret large transaction populations and identify unusual patterns, exceptions, and emerging risks. The paper further discusses implications for audit quality, professional skepticism, fraud-risk assessment, evidence evaluation, internal control monitoring, and the changing competencies of assurance professionals. At the same time, technological integration creates significant challenges involving legacy systems, privacy, cybersecurity, algorithmic bias, explainability, smart-contract risk, governance, regulatory uncertainty, and the reliability of technology-generated audit evidence. The paper argues that AI and blockchain should be viewed as complementary components of an assurance ecosystem rather than as substitutes for auditor judgment. The proposed framework provides a basis for future empirical research on implementation, audit efficiency, assurance quality, regulatory requirements, and the economic consequences of technology-enabled continuous auditing.

Keywords: Artificial Intelligence; Blockchain; Continuous Auditing; Audit Analytics; Machine Learning; Smart Contracts; Distributed Ledger Technology; Audit Automation

Introduction:

Digital transformation is reshaping the way organisations create, process, store, and communicate financial information. Accounting systems increasingly capture transactions electronically through enterprise resource planning (ERP) platforms, electronic invoicing, cloud applications, payment systems, Internet of Things (IoT) devices, and other connected technologies. The volume, velocity, and variety of information available to organisations have consequently expanded. Traditional auditing methods, although grounded in established principles of evidence, risk assessment, professional skepticism, and sampling, were largely designed for an environment in which transaction processing was slower and information was less continuously available. The

increasing digitisation of business therefore creates both an opportunity and a challenge for the assurance profession.

Artificial Intelligence (AI) and blockchain are two technologies with particularly strong relevance to this transformation. AI can process large datasets, recognise patterns, identify anomalies, classify information, generate predictions, and support decision-making. In auditing, these capabilities can be applied to journal-entry testing, fraud-risk assessment, contract analysis, document review, control monitoring, and substantive analytical procedures. Professional guidance from the International Auditing and Assurance Standards Board (IAASB) recognises that automated tools and techniques, including data analytics, robotics, and AI applications, are increasingly relevant to audit engagements (International Auditing and Assurance Standards Board [IAASB], 2020, 2022).

Blockchain contributes a different capability. It is a distributed ledger technology in which transactions can be recorded using cryptographic mechanisms and shared among authorised participants. In accounting and assurance, blockchain has been proposed as a mechanism for improving transaction traceability, reducing reconciliation requirements, and supporting more timely and verifiable accounting information (Dai & Vasarhelyi, 2017). Blockchain does not, by itself, guarantee that every transaction entered into a ledger is economically valid; rather, it can strengthen the integrity and traceability of the recorded information. This distinction is important for auditors because assurance concerns not only whether data have remained unchanged after recording, but also whether the underlying transactions are authorised, complete, accurate, properly classified, and supported by appropriate evidence.

The central proposition of this paper is that AI and blockchain have complementary strengths. Blockchain can function as a trusted record and evidence layer, while AI can operate as an analytical and cognitive layer. Their integration may allow auditors to examine transaction populations continuously, identify exceptions promptly, and focus professional judgment on higher-risk matters. Dai and Vasarhelyi (2017) argue that blockchain has the potential to support real-time, verifiable accounting and assurance, while Schmitz and Leoni (2019) identify significant implications of blockchain for accounting and auditing research and practice. The convergence of the two technologies therefore deserves examination as an integrated assurance model rather than as two independent innovations.

The purpose of this conceptual study is to develop a framework explaining how AI and blockchain can work together to support continuous assurance. The paper addresses three research questions: (1) How do AI and blockchain individually and collaboratively transform accounting and auditing workflows? (2) What architecture can integrate AI analytics with blockchain-backed transaction records for continuous assurance? and (3) What operational, technical, professional, ethical, and regulatory challenges may limit implementation?

Research Objectives and Methodological Approach:

The study has four objectives. First, it examines the individual contribution of AI and blockchain to accounting and auditing. Second, it analyses the potential synergy between AI-based analytics and blockchain-based transaction records. Third, it proposes a conceptual Continuous Assurance Architecture (CAA) that connects transaction generation, verification, analytics, and reporting. Fourth, it identifies implementation challenges and areas requiring further empirical investigation.

The paper follows a conceptual and literature-based approach. It builds on the ideas contained in the original manuscript and extends them through relevant academic and professional literature concerning AI, audit analytics, blockchain, continuous auditing, and technology-enabled assurance. The approach is not intended to provide statistical evidence of causal effects.

Accordingly, statements about improvements in audit efficiency, quality, or fraud detection are presented as conceptual possibilities or expected benefits rather than as empirically demonstrated outcomes of the proposed framework.

This methodological limitation is important. Technology adoption differs across organisations according to the maturity of information systems, transaction complexity, regulatory environment, governance structure, cybersecurity capabilities, and availability of skilled personnel. Therefore, the framework should be interpreted as a model for future empirical investigation rather than a claim that an integrated AI-blockchain system automatically produces high-quality audits.

Literature Review:

1. Artificial Intelligence in Accounting and Auditing: AI refers broadly to computational systems capable of performing tasks that normally require aspects of human intelligence, including perception, classification, language processing, pattern recognition, and decision support. In audit and assurance, AI can be applied across the audit lifecycle. The IAASB identifies AI as a significant technology affecting the audit and assurance value chain and describes applications involving risk assessment, document processing, anomaly detection, substantive procedures, and other audit activities (IAASB, 2022).

Machine learning can identify patterns in historical and current transaction data. Supervised learning can be trained using labelled examples, whereas unsupervised techniques can identify clusters or unusual observations without requiring every transaction to be pre-labelled. These approaches can support journal-entry analysis and fraud-risk assessment. Instead of restricting analysis to a relatively small sample, auditors may use technology to analyse larger populations and then investigate transactions or patterns that warrant attention.

Natural language processing (NLP) provides another important application. Accounting and auditing depend heavily on unstructured information, including contracts, invoices, emails, board minutes, regulatory documents, and policy manuals. NLP and related document-intelligence tools can extract clauses, dates, obligations, amounts, and other relevant information, thereby assisting auditors in understanding business processes and identifying potential accounting implications.

Automation can also reduce repetitive work. Robotic process automation (RPA) and related technologies can support data extraction, reconciliation, report preparation, and routine control procedures. However, automation should not be equated with the elimination of auditor responsibility. The IAASB notes that the use of automated tools affects how auditors perform and document procedures, while the underlying auditing standards and professional responsibilities remain applicable (IAASB, 2020).

2. Blockchain and Accounting Information: Blockchain provides a distributed method for recording transactions and maintaining a shared history among participating parties. Its relevance to accounting arises from the possibility of reducing information asymmetry and strengthening the traceability of transactions. Dai and Vasarhelyi (2017) propose that blockchain could support a real-time, verifiable, and transparent accounting ecosystem and could contribute to more timely assurance.

A blockchain-based environment can potentially reduce certain reconciliation activities because authorised participants may rely on a common transaction record. Cryptographic mechanisms and consensus processes can make unauthorised retrospective alteration more difficult. However, immutability should not be interpreted as proof of truth. If an incorrect or fraudulent transaction is validly recorded, the blockchain may preserve the incorrect record. Consequently, auditors still need to examine transaction initiation, authorisation, business context, controls, and relevant external evidence.

Smart contracts are another important component. Smart contracts are executable code stored on a blockchain that can automatically implement predetermined conditions. For

example, a contract could trigger a payment when specified delivery conditions are recorded. From an assurance perspective, the code itself becomes relevant evidence and a potential source of risk. An incorrectly designed smart contract can automate an incorrect business rule at scale. Auditors therefore need sufficient understanding of code logic, governance, access controls, and change-management procedures.

3. Continuous Auditing and Audit Analytics: Continuous auditing seeks to provide assurance activities closer to the time at which transactions and events occur. The development of data analytics has made it increasingly feasible to examine larger datasets and identify unusual patterns. Vasarhelyi, Kogan, and Tuttle (2015) describe how the growth of data and analytics can reshape auditing by enabling more extensive and timely analysis.

The movement toward continuous assurance does not necessarily mean that every audit procedure becomes permanently automated. Instead, continuous monitoring can provide an ongoing stream of risk information. Auditors may use dashboards, exception reports, automated alerts, and risk scores to identify matters requiring professional investigation. This can change the allocation of audit effort from routine verification toward higher-risk and judgment-intensive activities.

4. The Emerging Synergy Between AI and Blockchain: The potential value of integrating AI and blockchain arises from the complementary nature of the technologies. AI depends on the quality of its inputs, while blockchain can provide a consistent and traceable transaction history. At the same time, blockchain produces large amounts of transaction information that may be difficult to interpret manually, whereas AI can analyse those data rapidly.

The relationship should therefore be understood as complementary rather than deterministic. Blockchain can strengthen provenance and traceability, while AI can support interpretation, classification, anomaly detection, and prediction. The combination can potentially reduce the time between transaction occurrence, risk identification, and auditor response. However, the quality of the overall assurance outcome remains dependent on system design, governance, data quality, model performance, human oversight, and the relevance and sufficiency of audit evidence.

Proposed Conceptual Framework: Continuous Assurance Architecture:

The proposed Continuous Assurance Architecture (CAA) consists of four interconnected layers. The architecture extends the original manuscript's four-layer model while clarifying the responsibilities and assurance implications of each layer.

Layer 1: Data Ingestion and Transaction Generation: Transactions originate from ERP systems, point-of-sale systems, electronic invoicing platforms, banking interfaces, IoT devices, procurement systems, and other operational applications. At this stage, data quality is critical. The system should capture transaction identifiers, timestamps, participants, amounts, supporting documentation, authorisation information, and relevant metadata.

A key principle is that blockchain should not be treated as a replacement for all source systems. Instead, selected transaction information and evidence can be written to a permissioned distributed ledger according to predefined governance rules. Data validation at the point of entry can reduce duplicate, incomplete, or improperly formatted records. The architecture should also maintain links between ledger records and source documents so that auditors can trace transactions back to originating evidence.

Layer 2: Automated Verification and Blockchain Storage: In the second layer, transaction rules are automatically checked and validated. Smart contracts can perform predefined tests such as matching purchase orders with invoices, verifying approval thresholds, checking contractual conditions, or triggering predefined exceptions. Approved records can then be written to a permissioned blockchain.

This layer creates a tamper-evident transaction history. The objective is not simply to

make data immutable but to establish a traceable chain of events. Governance mechanisms should define who can create, approve, update, or access records. Because permissioned blockchain networks can restrict participation, they may be more appropriate than public blockchains for sensitive financial information.

Layer 3: AI-Based Cognitive Analysis and Anomaly Detection: The third layer represents the analytical core of the framework. AI models continuously analyse transaction streams and related information. Possible outputs include anomaly scores, fraud-risk indicators, unusual timing patterns, duplicate-payment alerts, unusual vendor behaviour, deviations from historical norms, and exceptions to accounting policies.

Different analytical techniques may be combined. Rules-based tests are appropriate for known control conditions; statistical techniques can identify deviations; supervised learning can support classification when labelled data are available; and unsupervised methods can identify previously unknown patterns. NLP can be applied to contracts and other unstructured information.

Model governance is essential. Each model should have defined objectives, documented inputs, validation procedures, performance thresholds, version controls, and escalation rules. Auditors should understand the limitations of model outputs and should not treat a high-risk score as proof of fraud.

Layer 4: Continuous Reporting and Decision Support: The fourth layer translates analytical results into information for auditors, management, audit committees, and other authorised stakeholders. Dashboards can display transaction volumes, exception trends, risk scores, control failures, unresolved alerts, and assurance indicators.

The purpose of continuous reporting is to support timely action. A significant anomaly identified shortly after a transaction occurs may allow management to investigate before the issue becomes widespread. Similarly, auditors may use recurring exception patterns to reassess risk, modify procedures, or evaluate the effectiveness of internal controls.

The architecture can therefore be represented as a continuous feedback loop: transaction generation leads to verification and recording; recorded information feeds AI analytics; analytical findings generate investigation and decision-making; and the results of investigations can improve controls and, where appropriate, future analytical models.

Transformation of the Auditing Process:

1. From Periodic Sampling to Population-Based Risk Analysis: Traditional audit approaches often rely on sampling because examining every transaction manually is impractical. AI-enabled analytics can make population-wide analysis more feasible. The auditor may analyse the entire population and investigate selected exceptions rather than selecting transactions only through conventional sampling.

This does not mean that statistical sampling becomes obsolete. Sampling may remain relevant where full-population testing is not technically appropriate or where the nature of the audit assertion requires procedures that cannot be automated. The important change is the expansion of the auditor's ability to examine data at scale.

2. Fraud Detection and Risk Assessment: AI can identify relationships and patterns that are difficult to detect through manual review. Examples include unusual combinations of vendor, employee, time, amount, location, and payment information. Blockchain can strengthen the traceability of transaction histories and reduce the possibility of unnoticed alteration after recording.

Nevertheless, fraud is fundamentally contextual. A transaction may appear unusual because of legitimate business circumstances, while sophisticated fraud may be designed to resemble normal activity. AI should therefore function as a risk-identification mechanism rather than a substitute for investigation and professional skepticism.

3. Internal Control Monitoring: Continuous monitoring can provide more timely information

about control performance. Automated tests can compare transactions against approval matrices, segregation-of-duties rules, contractual limits, and accounting policies. Repeated exceptions may indicate control deficiencies requiring management attention.

Blockchain can provide a traceable record of approvals and transaction events, while AI can analyse patterns in those records. Together, the technologies may help organisations move from periodic control testing toward more frequent monitoring.

4. Audit Evidence and Audit Trail: A major implication of the proposed framework is the transformation of the audit trail. In a traditional environment, auditors may assemble evidence from multiple systems and reconcile records. In an integrated environment, the ledger can provide a consistent transaction history while AI tools can organise and analyse supporting information.

However, the existence of a blockchain record does not automatically make the information sufficient appropriate audit evidence. Auditors must consider the reliability of the system, controls over access, the operation of consensus mechanisms, the integrity of data at entry, and the relationship between ledger records and underlying economic events. Technology can strengthen evidence, but it does not remove the need for evidence evaluation.

5. Professional Judgment and Skepticism: Automation may reduce routine tasks and enable auditors to devote more time to complex judgments. This can potentially strengthen professional skepticism if auditors use technology to investigate anomalies rather than merely accept automated results.

At the same time, excessive reliance on algorithms can create automation bias. Auditors may become less likely to challenge a system-generated conclusion. Therefore, the future auditor requires both technological literacy and traditional assurance skills. Understanding model limitations, interpreting outputs, challenging assumptions, and evaluating evidence will become increasingly important.

Benefits and Strategic Implications:

The integrated AI-blockchain model may generate several potential benefits.

First, efficiency can improve through automation of repetitive verification and data-processing activities. Auditors may spend less time obtaining, cleaning, reconciling, and manually testing routine transaction data.

Second, timeliness can improve. Continuous analytics can identify exceptions soon after transactions occur, enabling earlier investigation and remediation.

Third, audit coverage can expand. Where technology permits reliable analysis of entire transaction populations, auditors can identify patterns that might not be visible through conventional sampling.

Fourth, transparency and traceability can improve. Blockchain-based records can establish a chronological transaction history and reduce certain reconciliation problems among authorised participants.

Fifth, risk management can become more proactive. Predictive analytics can identify emerging risk indicators rather than restricting attention to historical misstatements.

Sixth, the role of the auditor can evolve. As routine activities become increasingly automated, auditors may focus more strongly on complex estimates, business-model risks, governance, controls, ethical issues, and interpretation of evidence.

These benefits are consistent with the broader direction of professional developments. The IAASB has stated that technology is increasingly intersecting with audit and assurance and that standards and guidance need to remain relevant as technologies evolve (IAASB, 2024). This indicates that technological adoption is not simply an operational matter for individual audit firms; it is also a standard-setting and professional-governance issue.

Challenges, Risks, and Limitations:

1. Legacy-System Integration: Many organisations operate heterogeneous and legacy systems. Connecting ERP platforms, accounting

applications, blockchain networks, data warehouses, and AI models can be technically complex. Integration costs may be particularly significant for small and medium-sized organisations.

2. Data Quality and the 'Garbage In, Garbage Out' Problem: Blockchain can protect the integrity of recorded information without guaranteeing the accuracy of the original input. If incorrect information enters the system, immutability may preserve the error. AI models are similarly dependent on data quality. Strong input controls, validation, master-data governance, and reconciliation mechanisms are therefore essential.

3. Algorithmic Bias and Explainability: AI models may produce false positives, false negatives, or biased results. Complex models may also be difficult for auditors and clients to explain. In assurance settings, explainability matters because auditors must be able to understand and document the basis for conclusions. Model governance should therefore include validation, monitoring, documentation, and appropriate human review.

4. Cybersecurity and Privacy: Financial information is highly sensitive. A blockchain implementation must protect confidentiality as well as integrity. Public blockchain designs may be unsuitable for confidential financial information, making permissioned networks and carefully designed access controls important. AI systems also introduce risks involving data access, model manipulation, third-party providers, and unauthorised use of sensitive information.

5. Smart-Contract Risk: Smart contracts can automate accounting and business rules, but coding errors may become automated control failures. Auditors may therefore need competencies in code review, change management, access control, and technology governance. Smart-contract assurance may emerge as a distinct area of professional practice.

6. Regulatory and Standards Uncertainty: Auditing standards were developed around fundamental principles that remain relevant, but the application of those principles to highly automated environments can create practical questions concerning evidence, documentation, model reliability, technology providers, and responsibility for automated procedures. The IAASB has been actively examining technology-related issues and has emphasised the need for standards to evolve with technological change (IAASB, 2024, 2026).

7. Skill Gaps: The integrated model requires professionals who understand accounting, auditing, information systems, data analytics, cybersecurity, and AI. Universities and professional bodies may therefore need to strengthen interdisciplinary education. Audit firms may also need multidisciplinary teams combining accountants with data scientists, technology specialists, cybersecurity professionals, and blockchain experts.

8. Human Oversight and Accountability: Automation should not obscure responsibility. When an AI model misses a fraudulent transaction or incorrectly flags a legitimate transaction, organisations must be able to identify who designed, approved, monitored, and relied upon the system. Clear accountability structures are essential for maintaining public trust.

9. Conceptual Nature of the Present Study: The paper is conceptual and does not provide primary empirical data. Consequently, the proposed benefits should not be interpreted as quantified outcomes. Future research should test the framework through case studies, experiments, surveys, and longitudinal implementation studies.

Governance Framework for Responsible AI-Blockchain Auditing:

A technology-enabled assurance system requires governance at multiple levels. At the organisational level, management should establish policies concerning system ownership, access rights, data quality, model approval, cybersecurity, and incident response. At the audit-firm level, technology used in an engagement should be subject to appropriate quality management, documentation, validation, and oversight.

Model governance should include at least five controls: clear definition of the model's purpose; documentation of data sources and assumptions; independent or appropriately robust validation; continuous monitoring of performance; and controlled model changes. These controls help ensure that AI outputs remain reliable and auditable.

Blockchain governance should address participant permissions, consensus mechanisms, cryptographic-key management, smart-contract approval, system updates, and recovery procedures. A permissioned blockchain may require formal rules for onboarding participants and resolving disputes.

Human-in-the-loop governance is particularly important. Automated alerts should be reviewed according to defined escalation criteria. Auditors should retain authority to challenge model outputs and perform additional procedures. The objective is not to replace professional judgment but to improve the information available for exercising it.

The governance framework should also distinguish between system reliability and audit evidence. Even when a technology platform operates as designed, auditors must consider whether the resulting information addresses the relevant assertion and whether it is sufficient and appropriate for the engagement. This distinction prevents technological sophistication from being mistaken for assurance quality.

Future Research Agenda:

The proposed framework creates several opportunities for empirical research.

First, researchers can conduct case studies of organisations implementing blockchain-enabled accounting systems with AI monitoring layers. Such studies could examine implementation costs, process changes, control effectiveness, and user acceptance.

Second, experimental studies can compare AI-supported audit procedures with conventional approaches. Measures could include detection rates, false-positive rates, time required, consistency of judgments, and the quality of documentation.

Third, future research can investigate the economic consequences of continuous assurance. Potential measures include audit hours, audit fees, reporting lag, control-remediation time, and the cost of technology implementation.

Fourth, research should examine how auditors interact with AI outputs. Questions include whether explainable models improve professional skepticism, whether automation bias occurs, and which forms of human review are most effective.

Fifth, researchers should study the assurance implications of smart contracts. This includes code auditing, change management, governance, and the relationship between smart-contract execution and accounting recognition.

Sixth, comparative studies across countries and regulatory environments can identify differences in technology adoption, privacy requirements, evidence rules, and professional competencies.

Finally, future research should examine whether AI and blockchain genuinely reduce audit risk or merely change its form. Technology may reduce certain risks, such as unauthorised alteration of recorded data, while creating new risks involving algorithms, cybersecurity, third-party systems, and model governance.

Conclusion:

The convergence of Artificial Intelligence and blockchain has the potential to reshape accounting and auditing by combining analytical intelligence with a more traceable and tamper-evident transaction environment. The central contribution of this paper is the proposed Continuous Assurance Architecture, which connects data generation, blockchain-based verification, AI-driven analysis, and continuous reporting.

The framework suggests a movement from predominantly retrospective and periodic audit activities toward more continuous, population-oriented, and risk-focused assurance. AI can support anomaly detection, predictive risk

analysis, document processing, and automated testing, while blockchain can strengthen transaction traceability and provide a shared record among authorised participants. Their combination can potentially reduce routine effort and allow auditors to concentrate on complex judgment, investigation, governance, and professional skepticism.

However, the technologies should not be viewed as automatic solutions to audit-quality problems. Blockchain does not guarantee the truthfulness of input data, and AI does not guarantee correct decisions. Both technologies introduce new risks relating to data quality, cybersecurity, privacy, algorithmic bias, explainability, smart contracts, system integration, and professional responsibility. The future of technology-enabled assurance therefore depends as much on governance and human competence as on technological capability.

The profession is already responding to these changes. The IAASB's continuing work on technology reflects the need for standards and guidance to remain relevant in an increasingly technology-enabled audit environment. The long-term direction is likely to involve greater use of automated tools, data analytics, AI, and distributed technologies, but the auditor's responsibility for evidence, judgment, ethics, and accountability remains central.

The proposed framework should consequently be understood as a conceptual foundation for future empirical investigation. Research that tests implementation outcomes, audit quality, efficiency, professional judgment, regulatory implications, and economic consequences will be necessary to determine the practical conditions under which AI-blockchain integration can deliver reliable continuous assurance.

References:

1. 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
2. International Auditing and Assurance Standards Board. (2020). Non-authoritative support material: Audit documentation when using automated tools and techniques. International Federation of Accountants.
3. International Auditing and Assurance Standards Board. (2022). IAASB digital technology market scan: Artificial intelligence—A primer. International Federation of Accountants.
4. International Auditing and Assurance Standards Board. (2024). Technology position. International Federation of Accountants.
5. International Auditing and Assurance Standards Board. (2026). Technology quality management roundtables: Outcomes and next steps. International Federation of Accountants.
6. 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.12286
7. Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big data in accounting: An overview. Accounting Horizons, 29(2), 381–396.
8. Yermack, D. (2017). Corporate governance and blockchains. Review of Finance, 21(1), 7–31. https://doi.org/10.1093/rof/rfw074
9. Coyne, J. G., & McMickle, P. L. (2017). Can blockchains serve an accounting purpose? Journal of Emerging Technologies in Accounting, 14(2), 101–111.