e-ISSN: 3025-8189 ; p-ISSN: 3025-8197

LANCAH JURNAL INOVASI DAN TREN

doi.org/10.35870/ljit.v4i2.8541

Vol. 4, No. 2, 2026

PP. 285-293

Homepage http://www.journal.lembagakita.com/ljit

The Influence of Blockchain Adoption on Audit Efficiency and Fraud Detection

Hadi Nurhadi[1], Mahdi[2], Irdawati[3], Meliana[4]

STIE Mulia Pratama[1,3]

Universitas Serambi Mekkah[2]

Universitas Khairun[4]

Corresponding Author's Email:hnhadi274@gmail.com

INFO ARTICLE:

History Article:

Submitted *08 20, 2026*

Received *08 26, 2026*

Published *08 30, 2026*

ABSTRACT

This article examines how the adoption of blockchain technology influences audit efficiency and fraud detection within modern accounting practice. As financial transactions increasingly move into distributed ledger environments, external auditors are compelled to revisit the assumptions, procedures, and tools that underpin traditional assurance work. Through a systematic review of contemporary auditing, accounting information systems, and financial technology literature, this study identifies the mechanisms through which blockchain reshapes the audit process. The findings indicate that blockchain adoption enhances efficiency primarily by enabling real-time access to immutable transaction records, reducing reliance on sampling-based procedures, automating control testing through smart contracts, and facilitating continuous auditing. At the same time, the technology strengthens fraud detection capacity by improving the traceability of transactions, increasing the difficulty of retroactive manipulation, and supporting forensic analysis of anomalous patterns. However, the realization of these benefits is conditional on several factors, including auditor competence, integration with legacy systems, regulatory clarity, data privacy constraints, and the risk that fraud shifts to points where the blockchain boundary intersects with off-chain processes. The review concludes that blockchain does not eliminate the need for professional skepticism; rather, it redefines the focus of auditor judgment from verifying recorded transactions to evaluating the reliability of the underlying technology environment and its governance. Practical implications for audit firms, standard-setting bodies, and regulators are discussed.

Keywords: *Blockchain; Audit Efficiency; Fraud Detection; Continuous Auditing; Financial Technology*

How to Cite:

Nurhadi, H., Mahdi, M., Irdawati, I., & Meliana, M. (2026). The Influence of Blockchain Adoption on Audit Efficiency and Fraud Detection. LANCAH: Jurnal Inovasi Dan Tren, 4(2), 285-293. https://journal.lembagakita.com/ljit/article/view/8541

INTRODUCTION

The auditing profession operates within a rapidly changing technological landscape in which the volume, velocity, and complexity of financial data continue to grow exponentially (Appelbaum et al., 2017; Dai & Vasarhelyi, 2017). Within this dynamic environment, traditional audit approaches that rely heavily on periodic testing and manual sampling are increasingly challenged. Today's auditors face a growing mandate to overcome these limitations and provide timely, continuous assurance over massive datasets that are constantly updating.

In response to these shifting demands, practitioners and scholars have actively turned their attention to emerging technologies capable of reshaping the audit landscape. Blockchain has received particular attention in this regard, largely due to its core promise of transparency, immutability, and decentralization (Yermack, 2017; Coyne & McMickle, 2017). As a distributed ledger technology, blockchain operates by grouping transactions into blocks that are cryptographically linked and validated by network participants before being permanently recorded.

Because these historical records are extremely difficult to alter retroactively without immediate detection, blockchain is frequently described as providing a secure, tamper-evident foundation for financial reporting (Tschorsch & Scheuermann, 2016; Zheng et al., 2018). These robust characteristics have led many observers to argue that the technology could fundamentally alter the audit paradigm. Specifically, there is widespread optimism that blockchain will revolutionize how auditors collect reliable evidence, evaluate internal controls, and proactively detect fraudulent activity (Bonyuet, 2020; Kokina et al., 2017).

At the same time, expectations regarding blockchain must be tempered by a realistic assessment of its limitations. The technology is not a universal solution to fraud, because fraud can still occur before data enters the ledger, through manipulation of off-chain systems, or through fraudulent initiation of transactions (Rozario & Vasarhelyi, 2018; Liu et al., 2019). Furthermore, the adoption of blockchain within organizations is uneven, and many companies operate hybrid environments in which blockchain modules coexist with conventional enterprise resource planning systems (Zhang et al., 2020; Schmitz & Leoni, 2019). These realities introduce significant complexity for auditors who must determine the extent to which they can rely on blockchain-generated evidence.

Despite growing interest, the literature on blockchain in auditing remains fragmented, and empirical evidence linking blockchain adoption to measurable improvements in audit efficiency and fraud detection is still emerging (Fuller & Markelevich, 2020; Lombardi et al., 2022). Many studies are conceptual or exploratory, and the conditions under which blockchain delivers its promised benefits are not yet fully understood. This article addresses that gap by synthesizing existing research and identifying the mechanisms, benefits, and constraints associated with blockchain-enabled auditing.

The purpose of this article is to provide a comprehensive analysis of the influence of blockchain adoption on audit efficiency and fraud detection. The review is organized as follows. First, the method used to synthesize the literature is described. Second, the results and discussion section examine several thematic dimensions of blockchain-enabled auditing. Third, the conclusion summarizes the key findings and outlines implications for practitioners and future research.

METHODS OF RESEARCH

This article employs a systematic literature review approach to examine the relationship between blockchain adoption, audit efficiency, and fraud detection. The review draws on scholarly articles published

in peer-reviewed journals, reputable conference proceedings, and authoritative industry reports within the fields of auditing, accounting information systems, and financial technology.

The literature search was conducted across major academic databases using keywords such as blockchain, distributed ledger technology, audit automation, continuous auditing, audit efficiency, fraud detection, and smart contracts. Studies were included if they addressed the application of blockchain within an auditing context, examined the implications of distributed ledger technology for evidence collection or internal control evaluation, or provided empirical or conceptual insights into fraud detection in blockchain environments.

The selected literature was analyzed thematically to identify recurring patterns, divergent perspectives, and unresolved questions. Cross-study comparison was used to distinguish findings that are widely supported from those that remain contested. Finally, the synthesized evidence was organized into thematic categories that reflect the main mechanisms through which blockchain influences audit efficiency and fraud detection. This narrative synthesis enables the formulation of implications that are relevant to audit practitioners, standard setters, and regulators.

RESULT AND DISCUSSION

Blockchain Adoption and the Transformation of Audit Efficiency

The first theme emerging from the literature concerns the capacity of blockchain to transform audit efficiency by changing the fundamental way in which audit evidence is accessed and processed. In traditional auditing, evidence collection is often a labor-intensive activity involving requests for documentation, manual reconciliation, and the physical or digital retrieval of supporting records (Appelbaum et al., 2017). Blockchain environments alter this dynamic because transaction data are recorded in a shared, structured, and continuously updated ledger that is accessible to authorized parties in near real time. This accessibility reduces the time auditors spend on data collection and enables them to devote greater attention to analysis and professional judgment (Dai & Vasarhelyi, 2017).

Table 1: Summary of Key Themes on the Impact of Blockchain on Audit Practice

Literature Theme	Main Impact / Mechanism	Challenges & Limitations
Audit Efficiency	Real-time data access, full population testing, automation of routine procedures, continuous auditing.	Organizational readiness, need for procedural adaptation, and quality of integration with legacy systems.
Fraud Detection	Data immutability, audit trail traceability across organizational boundaries, application of advanced analytics.	Early manipulation (before entering the ledger), off-chain system manipulation, and inability to prevent false origin.
Smart Contracts	Continuous automation of control testing, detailed visibility of execution logic.	Control quality depends on programming logic; risk of large-scale systematic flaws or bugs.
Barriers to Adoption	Shifts focus toward integration and regulatory navigation.	Lack of technical expertise (cryptography, smart contracts), legacy systems, regulatory & data privacy uncertainty.
New Assurance Model	Focus shifts from transaction verification to technology governance evaluation.	Requires a higher level of professional scepticism at system boundaries.

A particularly important consequence of blockchain adoption is the potential reduction in reliance on sampling-based audit procedures. When transactions are recorded on an immutable distributed ledger, auditors can theoretically examine the entire population of transactions rather than relying on statistically selected samples (Kokina et al., 2017). The ability to verify the full dataset, rather than a subset, has the potential to increase both the efficiency and the assurance value of substantive testing. This shift is especially relevant in organizations with high transaction volumes, where exhaustive verification would previously have been prohibitively expensive and time-consuming (Rozario & Vasarhelyi, 2018).

Efficiency gains are also realized through the automation of routine audit procedures. Smart contracts, which are self-executing agreements with terms encoded directly into the blockchain, can automate the verification of transactions against predefined business rules (Zheng et al., 2018). For example, a smart contract can automatically flag transactions that exceed approval thresholds, deviate from expected patterns, or fail to match underlying documentation. By automating these checks, auditors can redirect their effort toward higher-value activities such as evaluating unusual transactions and assessing the adequacy of management estimates (Schmitz & Leoni, 2019; Liu et al., 2019).

In addition, blockchain adoption supports the movement toward continuous auditing, in which assurance activities are performed on an ongoing basis rather than at discrete points in time (Vasarhelyi et al., 2004; Rozario & Thomas, 2019). Because blockchain provides a stable and continuously updated record of transactions, auditors can monitor key indicators and control activities in real time. Continuous auditing enables earlier identification of errors and anomalies, reduces the need for extensive year-end procedures, and improves the timeliness of assurance reports. The combination of real-time data access, complete population testing, automated controls, and continuous monitoring therefore forms a coherent pathway through which blockchain enhances audit efficiency (Bonyuet, 2020; Lombardi et al., 2022).

Nevertheless, the efficiency benefits of blockchain are not automatic and depend on the quality of integration with existing audit methodologies. Auditors must adapt their procedures, invest in new analytical tools, and develop the skills required to interrogate blockchain-based data (Fuller & Markelevich, 2020). Organizations that adopt blockchain in a fragmented manner, without aligning the technology with broader audit infrastructure, may fail to realize significant efficiency gains. Thus, while blockchain presents considerable potential to streamline the audit process, its impact on efficiency is mediated by organizational readiness and the maturity of supporting systems (Zhang et al., 2020).

Immutability, Traceability, and the Enhancement of Fraud Detection

The second theme addresses the influence of blockchain on the capacity of auditors to detect fraudulent activity. The most frequently cited mechanism in this regard is the immutability of the distributed ledger. Because records on a blockchain are cryptographically linked and difficult to alter without network consensus, the opportunity for retrospective manipulation of financial records is substantially reduced (Tschorsch & Scheuermann, 2016; Yermack, 2017). This characteristic strengthens the reliability of the underlying data and increases the likelihood that intentional misstatements will be detected or deterred. Blockchain also enhances fraud detection through improved traceability. Each transaction recorded on the ledger is associated with a permanent audit trail that documents its origin, destination, and validation history (Zheng et al., 2018). This traceability is particularly valuable in complex supply chains and multi-entity transactions, where the movement of funds or goods can be followed from initiation to settlement. Auditors can leverage this trail to reconstruct the economic substance of transactions, identify discrepancies between

recorded entries and actual events, and investigate transactions that cross organizational boundaries (Coyne & McMickle, 2017; Appelbaum et al., 2017).

The structured and standardized nature of blockchain data further supports the application of advanced analytical techniques in fraud detection. Machine learning algorithms and anomaly detection tools can be applied to the complete transaction population to identify unusual patterns, clustering behaviors, or deviations from expected norms (Liu et al., 2019; Lombardi et al., 2022). Because blockchain provides clean, consistent, and machine-readable data, the quality of analytical models improves, and the speed with which anomalies are surfaced increases. This capability aligns with the broader trend toward data-driven auditing and forensic analytics in the accounting profession (Rozario & Thomas, 2019).

However, it is essential to recognize the boundaries of blockchain in fraud prevention. Fraud can still occur at the point of transaction origination, where an authorized party intentionally records a false transaction that is subsequently validated by the network (Bonyuet, 2020). Similarly, manipulation of systems that interface with the blockchain, such as off-chain databases or legacy applications, may create discrepancies that are not visible within the ledger itself (Schmitz & Leoni, 2019). Consequently, blockchain changes the location and nature of fraud risk rather than eliminating it entirely, and auditors must design procedures that address risks at the intersection of blockchain and conventional systems (Rozario & Vasarhelyi, 2018).

The implications of these findings for fraud detection are twofold. First, blockchain strengthens the evidentiary value of transaction data, making it more difficult for fraud to persist undetected once it has entered the ledger. Second, the technology demands that auditors expand their attention to include the governance of the blockchain environment, the integrity of interfaces, and the reliability of the parties responsible for initiating transactions. Fraud detection in a blockchain environment therefore requires a combination of technological capability, analytical skill, and enhanced professional skepticism (Fuller & Markelevich, 2020; Kokina et al., 2017).

Smart Contracts and the Automation of Control Testing

The third theme concerns the role of smart contracts in transforming the evaluation of internal controls. Internal control assessment is a fundamental component of the audit process, and traditional approaches often involve manual testing of control activities to determine whether they operate effectively (Vasarhelyi et al., 2004). Smart contracts provide a mechanism through which control rules can be embedded directly into transaction processing, allowing controls to be enforced automatically and continuously (Zheng et al., 2018; Liu et al., 2019).

From an audit perspective, the automation of controls has two significant implications. First, it reduces the extent to which auditors must rely on after-the-fact testing, because the operating effectiveness of automated controls can be observed directly from the blockchain (Schmitz & Leoni, 2019). Second, it enables auditors to assess control performance across the entire population of transactions, rather than sampling individual instances. The resulting improvement in the reliability of control evidence enhances both the efficiency and the effectiveness of the audit process (Dai & Vasarhelyi, 2017).

The transparency of smart contract execution also supports the identification of control weaknesses. Because the logic and execution of smart contracts are visible to authorized parties, auditors can review the precise conditions under which transactions are approved, rejected, or escalated (Bonyuet, 2020). This visibility allows auditors to detect gaps in the design of controls, to evaluate whether automated approvals

are consistent with policy, and to identify situations in which control exceptions are systematically overlooked (Rozario & Thomas, 2019).

Despite these advantages, the reliance on smart contracts introduces new audit risks. The quality of automated controls is only as good as the logic embedded within the contract, and programming errors or design flaws can lead to systematic failures that affect large volumes of transactions (Tschorsch & Scheuermann, 2016; Yermack, 2017). Auditors must therefore evaluate not only the operation of smart contracts but also the rigor of their development, testing, and governance. The emergence of specialized expertise in blockchain controls suggests that audit teams will need to combine accounting knowledge with technical competence in distributed systems (Fuller & Markelevich, 2020).

In summary, smart contracts offer a compelling pathway for automating control testing and enhancing the efficiency of internal control evaluation. Nevertheless, their introduction demands a sophisticated approach to audit risk assessment, in which the reliability of automated logic is treated as a subject of audit evidence in its own right. The future of control testing in blockchain environments will likely be characterized by a partnership between automated monitoring and professional judgment (Zhang et al., 2020; Lombardi et al., 2022).

Barriers to Adoption: Skills, Legacy Systems, and Regulatory Uncertainty

The fourth theme examines the obstacles that limit the realization of blockchain benefits within audit practice. One of the most significant barriers is the shortage of auditors who possess the technical skills required to understand blockchain architecture, evaluate distributed ledger controls, and interpret blockchain-based evidence (Bonyuet, 2020; Fuller & Markelevich, 2020). The auditing profession has traditionally drawn on accounting and financial expertise, and the integration of cryptography, consensus mechanisms, and smart contract logic into the auditor skill set represents a substantial educational and professional development challenge.

A second barrier is the coexistence of blockchain systems with legacy information technology infrastructure. Many organizations operate hybrid environments in which blockchain modules must interface with conventional enterprise resource planning and accounting systems (Zhang et al., 2020). Data inconsistencies between these systems, the need for middleware and integration layers, and the absence of standardized data formats create significant complexity for auditors seeking to obtain a complete and reliable view of the organization (Schmitz & Leoni, 2019). Until integration challenges are resolved, the full benefits of blockchain in auditing are unlikely to be achieved.

Regulatory uncertainty represents a third and particularly important barrier. The legal and regulatory status of blockchain records, the enforceability of smart contracts, and the treatment of digital assets within financial reporting frameworks remain unsettled in many jurisdictions (Yermack, 2017; Coyne & McMickle, 2017). Auditors require clear guidance on the extent to which blockchain evidence can be relied upon, the documentation requirements associated with distributed ledgers, and the responsibilities of auditors when technology failures occur. In the absence of such guidance, audit firms may adopt cautious approaches that limit the efficiency gains that blockchain could otherwise deliver (Liu et al., 2019).

Data privacy and confidentiality concerns also constrain the application of blockchain in auditing. Because blockchain networks may replicate data across multiple nodes, the storage of sensitive financial information raises questions regarding data protection, access control, and compliance with privacy regulations (Appelbaum et al., 2017; Tschorsch & Scheuermann, 2016). Auditors must navigate these

concerns when accessing or analyzing blockchain data, and the design of private or permissioned ledgers becomes an important consideration in balancing transparency with confidentiality (Zheng et al., 2018).

Taken together, these barriers suggest that blockchain adoption in auditing is likely to proceed gradually and unevenly. Organizations with mature technology governance, substantial investment capacity, and access to specialized talent are better positioned to realize the benefits of blockchain, while smaller firms and organizations in developing regulatory environments may experience delayed adoption (Fuller & Markelevich, 2020). Understanding these constraints is essential for developing realistic expectations regarding the pace and scope of blockchain-enabled auditing (Rozario & Thomas, 2019).

Redefining the Assurance Model: Technology Governance and Professional Skepticism

The fifth theme explores the broader implications of blockchain for the assurance model and the role of professional judgment. A recurring conclusion in the literature is that blockchain does not render the auditor obsolete; rather, it repositions the focus of audit work (Kokina et al., 2017; Lombardi et al., 2022). When transaction records are reliable and complete, the auditor attention shifts from verifying individual transactions to evaluating the environment in which those transactions were created and validated (Rozario & Vasarhelyi, 2018).

This reorientation places greater emphasis on the governance of the blockchain environment. Auditors must assess the adequacy of controls over network access, the integrity of consensus mechanisms, the reliability of node operators, and the policies governing the initiation of transactions (Schmitz & Leoni, 2019). The quality of the technology environment becomes, in effect, a subject of audit evidence, and the auditor evaluation of that environment determines the extent to which reliance can be placed on blockchain records (Dai & Vasarhelyi, 2017).

Professional skepticism remains a cornerstone of the audit profession, and its importance is amplified in blockchain environments rather than diminished. Auditors must question assumptions about the reliability of technology, investigate anomalies that may indicate fraud, and resist the temptation to place undue confidence in automated records simply because they are difficult to alter (Fuller & Markelevich, 2020). The persistence of fraud risks at the boundaries of blockchain, including off-chain manipulation and fraudulent transaction initiation, requires auditors to maintain a questioning mindset throughout the engagement (Bonyuet, 2020).

The evolution of the assurance model also has implications for the relationship between auditors and the organizations they serve. Continuous auditing enabled by blockchain may support more timely communication of findings, earlier identification of emerging risks, and closer collaboration between management and auditors (Vasarhelyi et al., 2004). At the same time, the expanded scope of technology governance raises questions regarding the division of responsibility between management, internal audit, and external auditors, and the extent to which auditors can rely on the work of technology specialists (Zhang et al., 2020).

Ultimately, the literature suggests that blockchain is best understood not as a replacement for professional judgment but as a transformation of its application. The auditor of the future will combine analytical capability with technical understanding, applying professional skepticism to both the data and the systems that generate it. The successful integration of blockchain into the assurance model will therefore depend on the ability of the profession to adapt its standards, education, and methodologies to a technologically sophisticated environment (Coyne & McMickle, 2017; Lombardi et al., 2022).

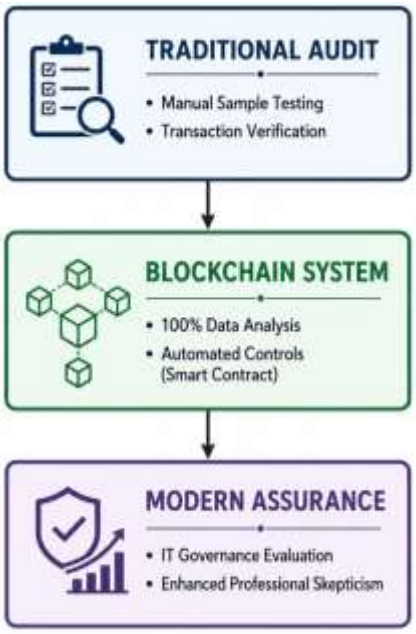

Figure 1. Paradigm Shift in the Audit Assurance Model via Blockchain

CONCLUSION

This article has examined the influence of blockchain adoption on audit efficiency and fraud detection. The review demonstrates that blockchain offers significant potential to enhance audit efficiency by enabling real-time access to transaction data, supporting full-population testing, automating routine procedures through smart contracts, and facilitating continuous auditing. The technology also strengthens fraud detection by improving the immutability and traceability of records and by enabling sophisticated analytical techniques to be applied to complete and reliable datasets.

At the same time, the realization of these benefits is conditional on a range of organizational, technical, and regulatory factors. Auditor competence, the integration of blockchain with legacy systems, regulatory clarity, data privacy constraints, and the governance of the blockchain environment all shape the extent to which blockchain delivers its promised advantages. Furthermore, blockchain changes the nature of fraud risk rather than eliminating it, and professional skepticism remains essential in evaluating both the technology and the transactions it records.

The findings carry important implications for audit firms, standard-setting bodies, and regulators. Audit firms should invest in the development of technical skills and analytical capabilities required for blockchain-enabled auditing. Standard setters should provide clear guidance on the reliance that may be placed on blockchain evidence and on the documentation of technology governance. Regulators should work toward greater clarity regarding the legal status of blockchain records and smart contracts. Future research should examine blockchain-enabled auditing through empirical studies, including investigations of adoption in diverse organizational settings and the development of frameworks for assessing the reliability of blockchain environments.

REFERENCES

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). An introduction to data analysis for auditors and accountants. Auditing: A Journal of Practice & Theory, 36(4), 1-13. https://doi.org/10.2308/ajpt-51762

Bonyuet, D. (2020). Blockchain: A new paradigm for auditing. Journal of Emerging Technologies in Accounting, 17(1), 35-43. https://doi.org/10.2308/jeta-2020-007

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

Fuller, S. H., & Markelevich, A. (2020). The impact of blockchain on the audit profession. Journal of Emerging Technologies in Accounting, 17(1), 45-58. https://doi.org/10.2308/jeta-2020-008

Kokina, J., Mancha, R., & Pachamanova, D. (2017). Blockchain: Emergent industry adoption and implications for accounting. Journal of Emerging Technologies in Accounting, 14(2), 91-100. https://doi.org/10.2308/jeta-51911

Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting? Permissionless versus permissioned blockchain. Journal of Emerging Technologies in Accounting, 16(2), 15-31. https://doi.org/10.2308/jeta-52540

Lombardi, R., de Villiers, C., Mio, C., & Vasarhelyi, M. A. (2022). The disruption of blockchain in auditing: A literature review and research agenda. Accounting, Auditing & Accountability Journal, 35(7), 1534-1555. https://doi.org/10.1108/AAAJ-10-2020-4992

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-52411

Rozario, A. M., & Vasarhelyi, M. A. (2018). Auditing with smart contracts. International Journal of Digital Accounting Research, 18, 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.12286

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. Journal of Emerging Technologies in Accounting, 1(1), 1-21. https://doi.org/10.2308/jeta.2004.1.1.1

Yermack, D. (2017). Corporate governance and blockchains. Review of Finance, 21(1), 7-31. https://doi.org/10.1093/rof/rfw074

Zhang, Y., Wen, J., & Xiong, F. (2020). Blockchain and audit: A review and research agenda. Journal of Accounting and Public Policy, 39(5), 106745. https://doi.org/10.1016/j.jaccpubpol.2020.106745

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375. https://doi.org/10.1504/IJWGS.2018.095647