Auditing Blockchain Innovations: Technical Challenges Beyond Traditional Finance

Shayan Eskandari*
Leid Zejnilovic*
Jeremy Clark†
*Nova School of Business and Economics, Universidade NOVA de Lisboa,
Campus de Carcavelos, 2775-405 Carcavelos, Portugal
{shayan.eskandari, leid.zejnilovic}@novasbe.pt
†Concordia University, Montreal, Canada
j.clark@concordia.ca

***Abstract*—Blockchain technology introduces asset types and custody mechanisms that fundamentally break traditional financial auditing paradigms. This paper presents an autoethnographic analysis of cryptoasset auditing challenges, build on top of prior research on a comprehensive framework addressing existence, ownership, valuation, and internal control verification. Drawing from lived experience implementing blockchain systems as an engineer, smart contract auditor, and CTO of a publicly traded cryptoasset firm, we demonstrate how autoethnographic methodology becomes necessary for understanding technical complexities that external analysis cannot capture. Through detailed examination of token airdrops, multi-signature smart contracts, and real-time on-chain reporting, we provide experimental approaches and common scenarios that auditing firms can analyze to address blockchain innovations currently considered technically insurmountable.**

***Index Terms*—blockchain auditing, cryptoassets, autoethnography, smart contracts, financial audits, multi-signature, internal controls, ownership verification**

I. Introduction

The $4 trillion blockchain industry faces a critical barrier: major auditing firms refuse to certify companies holding significant cryptoassets, leading to cease trade orders and blocked access to capital markets [1], [2]. This reluctance stems from blockchain innovations that introduce fundamental paradigm shifts requiring entirely new audit procedures.

Unlike incremental technological changes accommodated within traditional procedures, blockchain creates new asset categories: tokens appearing without purchase transactions (airdrops), ownership structures without private key control (multi-signature smart contracts), and continuous financial reporting from immutable ledgers [3], [4]. These innovations break traditional audit frameworks designed for centralized systems with clear ownership documentation [5] and authorized (financial) statements.

Recent industry examples demonstrate the severity of this challenge. Several crypto companies, including those operating in regulated environments, were placed on cease trade orders when auditors abruptly stepped down, leaving firms unable to find replacement auditors [6], [7]. Even major exchanges like Binance have struggled to obtain audit certifications for proof-of-reserves procedures [8].

The Necessity of Autoethnographic Methodology. Traditional external audit analysis fails to capture the subtle technical dependencies that impact financial verification procedures. Consider multi-signature smart contracts: external observation might classify these as ”complex custody arrangements,” but only hands-on implementation reveals that ownership verification requires analyzing contract source code (often bytecode), validating governance mechanisms, and assessing upgrade risks—procedures with no traditional audit equivalent.

This paper employs autoethnographic methodology [9] to analyze blockchain audit challenges through lived professional experience across multiple industry roles. This approach is justified by the technical impossibility of understanding these systems without implementation experience [10], [11].

II. Methods

We adopt an applied research approach with theory-building perspective, addressing practical issues as they emerge and suggesting potential solutions [12]. This methodology combines systematic analysis with personal professional experience to bridge the knowledge gap between technical blockchain expertise and financial auditing requirements.

Professional Context: The analysis draws from lived experience of one of the authors and their progression through multiple blockchain ecosystem roles: (1) *Blockchain Engineer* providing foundational understanding of cryptocurrency transaction flows and key management; (2) *Smart Contract Security Auditor* revealing technical complexities requiring domain-specific expertise; (3) *Chief Technology Officer* exposing the disconnect between technical implementation and financial reporting requirements through direct auditor interaction.

Case Study Methodology: We employ paradigmatic case research [13] to examine specific blockchain innovations that fundamentally challenge traditional audit frameworks. This approach provides information about situations auditors face when attempting to verify emerging cryptoasset types and custody mechanisms. Three illustrative cases are analyzed: (1) token airdrop existence verification challenges; (2) self-custody ownership evolution; and (3) real-time blockchain-based financial reporting. Each case study combines technical

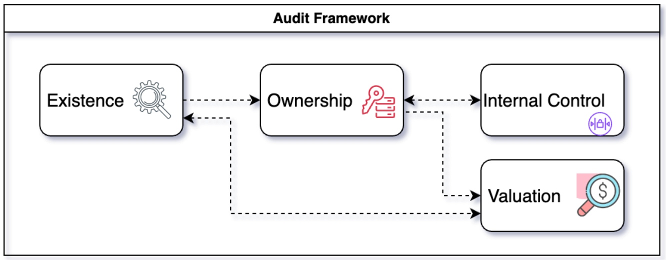


Fig. 1. Cryptoasset Audit Framework: A cryptoasset exists when it has material value and is owned by an entity. Ownership requires internal control to keep assets safe and accessible.

implementation details with autoethnographic analysis of auditor interactions, revealing systematic gaps between traditional audit procedures and blockchain innovation requirements. The research team combines ”complete participation” for technical implementation with ”observer participant” analysis, balancing insider insights with external academic perspective [14].

Table I summarizes the autoethnographic data sources informing this analysis. We employ evocative autoethnography [9] to capture lived experience of navigating technical-financial boundaries that external analysis cannot access, revealing implicit knowledge embedded in professional practice.

Autoethnographic Validation: Following established practice for single-researcher autoethnography, we employed systematic triangulation through the industry engagement documented in Table I. Conference presentations (10+ across security auditing contexts), regulatory workshops (5+ with compliance teams), and direct auditor engagements (2 annual audits and 6 quarterly reporting cycles) provided opportunities to test emerging insights against the experiences of other blockchain-audit interface practitioners. This validation process revealed consistent patterns across different organizational contexts, supporting the transferability of our autoethnographic findings [9]. The framework’s resonance with industry practitioners—from technical auditors to regulatory compliance teams—provided external validation of insights derived from personal professional experience spanning over 4000 hours of protocol auditing and $100M+ in assets under management.

III. Cryptoasset Audit Framework

Our autoethnographic analysis organizes blockchain audit challenges into four interconnected categories (Figure 1), extending prior work [1] with practical implementation insights.

A. Existence Challenges

Technical Innovation Impact: Blockchain creates assets through mechanisms that have no traditional acquisition equivalents. Token airdrops create assets appearing in company wallets without purchase transactions, delivery mechanisms, or counterparty relationships [15].

Reliability Assessment: Not all blockchain-based systems provide equivalent existence assurance. Auditors must evaluate consensus mechanism robustness, validator diversity, community support, cryptographic security [16], and system implementation. Bitcoin and Ethereum enjoy extensive validation, while obscure tokens may reside on unreliable networks.

Fork and Airdrop Complications: Existing accounting standards cannot accommodate non-reciprocal asset transfers [17]. The Ethereum merge or Bitcoin Cash fork, resulted in the creation of separate holdings on the blockchain forks [18], [19], while Optimism airdrops required complex claiming procedures with technical dependencies [20].

B. Ownership Verification

Self-Custody Challenges: Absent legal registers or official documents, auditors must rely on cryptographic proof systems. Ownership verification requires temporal considerations—proving control at fiscal year-end rather than audit date—and understanding the distinction between access and ownership [21].

Smart Contract Complexity: Multi-signature contracts implement governance mechanisms, upgrade procedures, and access controls with no traditional custody equivalent [22]. Unlike single key accounts (EOA), smart contracts require code analysis and governance validation [23].

Custodial Arrangements: Third-party custody requires evaluating Service Organization Control (SOC) reports, but these often inadequately address cryptoasset-specific controls [24]. Auditors must assess custodian segregation practices and technical implementation details.

C. Valuation Complexities

Market Fragmentation: Cryptoasset markets operate continuously across jurisdictions with fragmented liquidity and geographical price variations [25]. IFRS requirements for principal market identification become complex when trading occurs on multiple decentralized platforms [26].

Fungibility Issues: Digital assets introduce fungibility challenges unknown in traditional finance. ”Dirty” coins with histories involving in hacking incidents or privacy protocols like Tornado Cash may trade at discounts, creating valuation complexities [27], [28].

D. Internal Control Innovation

Technical Control Requirements: Effective cryptoasset internal controls require understanding hardware security modules (HSM), multi-signature threshold selection, secure key generation, and backup procedures. [29].

Control Trade-offs: More secure controls (multi-signature wallets) complicate ownership verification, while simpler approaches (single keys) create single points of failure. Auditors must evaluate these technical trade-offs without established time-tested frameworks [30].

IV. Auditing Challenges on Blockchain Innovations

A. Case Study 1: Airdrop Existence Verification

Technical Challenge: The Optimism airdrop required individual claiming transactions from each multi-sig keyholder,

TABLE I
AUTOETHNOGRAPHIC DATA SOURCES OVERVIEW: PROFESSIONAL EXPERIENCE

Experience Category	**Quantitative Scope**	**Time Period**	**Autoethnographic Analysis Focus & Insights**
Blockchain Engineering: Bitcoin ATM & Cloud Wallet Management	• 1000+ ATM deployments • $1B+ transaction volume	2015–2018	• Understanding Bitcoin operational complexity • Key management practical challenges • Gaps between theoretical security & implementation requirements
Smart Contract Security Auditing: DeFi protocol assessments	• 50+ protocol audits • 4000+ total audit hours • 10 conference presentations	2018–2021 2023–2025	• Technical complexity assessment methodologies • DeFi vulnerability identification • Code analysis procedures & audit frameworks • Domain-specific expertise requirements
Chief Technology Officer: Publicly-traded cryptoasset firm	• $100M+ AUM • 2 annual audit engagements • 6 quarterly financial statements • 15 airdrop claims • 5 regulatory workshops	2021–2023	• Direct auditor interaction experiences • Financial reporting integration challenges • Institutional custody complexities • Auditor knowledge gaps and cultural resistance • DeFi risk assessment challenges
Multisignature Implementation: Organizational custody	• 10+ multisig deployments • 12 governance configurations	2019–2025	• Governance mechanism design trade-offs • Control framework development insights • Technical custody evolution impact on audits

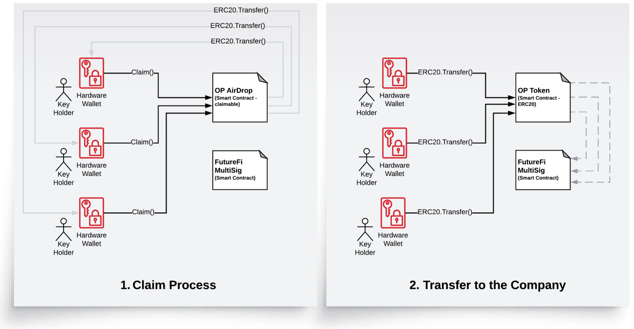


Fig. 2. Case Study 1 - Optimism Airdrop First Claim Workflow for Multi-signature Custody

with gas costs paid separately, creating complex technical dependencies (Figure 2) [20].

Autoethnographic Analysis: Managing 15 airdrop claims across multiple protocols revealed that these events often occur without notification, require protocol-specific claiming procedures, and involve technical risks that can jeopardize existing holdings. The moment I realized traditional auditing had no framework for airdrops came during our first quarterly audit when auditors requested ”purchase documentation” for tokens that had simply appeared in our wallets. This disconnect—between their need for acquisition evidence and the reality of permissionless token distribution—revealed the fundamental inadequacy of traditional audit frameworks. Multi-phase airdrops (Optimism had two phases) require different procedures for each phase, with gas costs varying by network congestion and claiming complexity. The lived experience of repeatedly explaining blockchain mechanics to confused auditors across 6 quarterly reporting cycles illustrated the persistent cultural and knowledge gap that autoethnographic analysis can bridge [9]. Each airdrop presented unique verification challenges: some required snapshot proofs, others involved staking requirements, and several had time-sensitive claiming windows that created additional audit timing complications.

Auditing Challenges: Traditional audit procedures cannot verify these technical dependencies. Instead, auditors must develop experimental approaches to confirm airdrop existence, ownership, and claiming procedures, as well as conduct gas cost-based analysis for valuing the airdropped tokens.

B. *Case Study 2: Multi-Signature Ownership Evolution*

Innovation Problem: A company evolved from single hardware wallet storage to multi-signature smart contract custody, fundamentally altering ownership verification requirements.

Technical Implementation: A single (hardware) wallet can sign a message with private keys to prove ownership, however, a smart contract does not have a private key to sign a message. Multi-signature Smart contracts implement complex governance requiring: (1) Source code analysis validating contract functionality; (2) Signatory verification ensuring keyholders possess claimed keys; (3) Governance mechanism assessment evaluating upgrade risks; (4) Emergency procedure evaluation understanding recovery mechanisms.

Autoethnographic Analysis: Implementing many self custody solutions across 12 different governance configurations over six years revealed the profound evolution of custody paradigms. When auditors requested ”proof of ownership,” I realized I couldn’t simply demonstrate private key control—the very concept of ownership had evolved beyond traditional frameworks. Each multisig configuration presented unique verification challenges: 2-of-3 setups required different governance documentation than DAO (Decentralized autonomous organization) arrangements, and emergency recovery procedures varied dramatically based on keyholder distribution and organizational structure. The embodied experience of coordinating multiple keyholders for routine transactions—from simple transfers to complex smart contract interactions—revealed the inadequacy of existing audit procedures. This lived complexity spanning governance design trade-offs (security versus operational efficiency), technical custody evolution (key-based to smart contract-based), and control framework development could only be understood

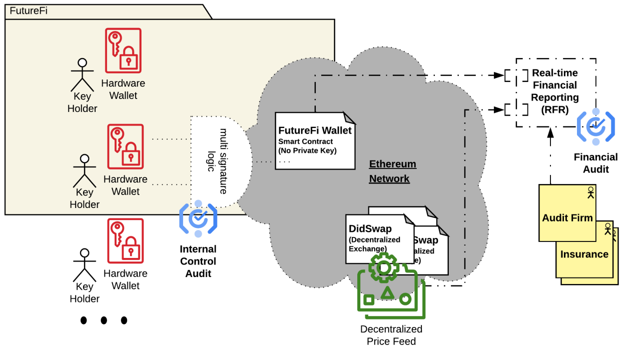


Fig. 3. Case Study 3 - Real-time Financial Reporting (RFR): Blockchain transparency enables continuous audit verification but requires new control frameworks.

through direct implementation across multiple organizational contexts, not external observation [9].

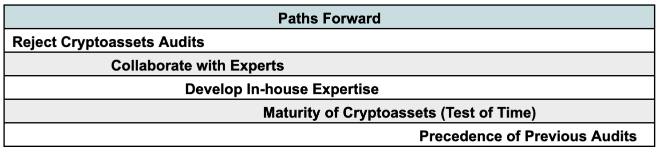
Auditing Challenges: Auditors must develop technical expertise to analyze implementation and define ownership verification procedures. This requires understanding cryptographic primitives and network operations that traditional audits do not address [29].

C. Case Study 3: Real-time Financial Reporting

Technical Innovation: This experimental system enables auditors to verify asset quantities directly from blockchain nodes and obtain valuations from decentralized price feeds [31], eliminating reliance on client-provided information (Figure 3) [32].

Autoethnographic Analysis: Proposing this solution during the last annual audit engagement covering $100M+ in assets under management revealed that traditional auditors are not equipped with the technical expertise to feel comfortable with cryptographically verifiable data from the blockchain [33]. The resistance I encountered when demonstrating real-time blockchain verification to our auditors was visceral and immediate. Despite providing mathematically verifiable proof of our holdings directly from blockchain nodes—data more reliable than traditional bank confirmations—they insisted on client-provided statements and manual reconciliation processes. This pattern repeated across multiple reporting periods: auditors would request CSV exports of on-chain data rather than verify it directly, creating additional points of failure and reducing audit quality. The cultural chasm between blockchain's inherent transparency and traditional audit culture's reliance on trusted intermediaries became most apparent during our year-end audits, where auditors questioned the integrity of immutable blockchain data while accepting mutable bank statements. The lived experience of managing financial reporting integration challenges—being simultaneously more transparent and less trusted—revealed the deep institutional inertia that autoethnographic analysis helps illuminate [9].

Control Framework Requirements: The approach requires new internal controls for: oracle security and redundancy, node infrastructure protection, automated reporting system integrity, and real-time monitoring mechanisms [34].



Paths Forward
Reject Cryptoassets Audits
Collaborate with Experts
Develop In-house Expertise
Maturity of Cryptoassets (Test of Time)
Precedence of Previous Audits

Fig. 4. Paths Forward for Auditing Cryptoassets

V. Discussion and Implications

Methodological Contributions: This research demonstrates that autoethnographic methodology is essential for understanding technical innovations that break existing paradigms. The lived experience of implementing blockchain systems provides insights that external analysis cannot generate [35], [36].

Figure 4 shows how auditing firms are evolving approaches to blockchain challenges. Our analysis reveals multiple pathways forward [37].

Collaboration with Experts: Successful implementations combine traditional audit expertise with blockchain security. Research shows relationship quality between auditors and IT specialists impacts audit evidence quality [38], [39].

Developing In-house Expertise: Major firms are creating specialized blockchain audit capabilities [40], [41]. However, this requires significant investment and competition for limited blockchain expertise [42].

Test of Time: As cryptoassets mature, more institutions recognize their relevance [43]–[45]. Regulatory clarity is emerging, with frameworks developing for cryptoasset treatment [46], [47].

Standards Development: Integration of traditional audit standards with cryptoasset security standards (like C4 CCSS) could create comprehensive frameworks [29]. Proof-of-reserves methodologies are evolving into standardized procedures [48], [49].

VI. Limitations and Future Work

Scope Limitations. This analysis focuses on specific blockchain innovations experienced through professional implementation. Different technical pathways might reveal additional challenges requiring experimental approaches [50]. The framework addresses traditional corporate entities holding cryptoassets but requires extension for decentralized autonomous organizations (DAOs).

Methodological Extensions. Future work should extend autoethnographic analysis to emerging innovations like zero-knowledge proofs, cross-chain protocols, and novel governance structures presenting new verification challenges [51].

Industry Validation. Broader implementation across different auditing contexts will validate framework applicability and reveal additional technical dependencies requiring systematic approaches.

VII. Conclusion

Blockchain innovations create fundamental challenges for traditional financial auditing requiring experimental approaches guided by technical understanding of the underlying technology and requirements. Token airdrops, multi-signature wallets, smart contracts, and real-time on-chain reporting represent paradigm shifts that existing frameworks cannot accommodate.

This research demonstrates the necessity of novel interdisciplinary methodologies for understanding technical innovations and breaking existing paradigms. Our approach provides a model for systematically analyzing emerging technologies requiring experimental verification, offering auditing firms pathways to address blockchain innovations rather than avoiding them entirely.

Acknowledgment

This work was funded by Fundação para a Ciência e a Tecnologia (UID/00124/2025, UID/ PRR/124/2025, Nova School of Business and Economics DOI: https://doi.org/10.54499/ UID/00124/2025) and LISBOA2030 (DataLab2030 - LISBOA2030-FEDER-01314200). It also received support from the University Blockchain Research Initiative (UBRI), funded by the Ripple Impact Fund under grant 2022-310159 (251937), awarded to the Data, Operations & Technology Knowledge Center (DOT KC), Nova School of Business and Economics, Universidade NOVA de Lisboa, Campus de Carcavelos, 2775-405 Carcavelos, Portugal

References

[1] E. Pimentel, E. Boulianne, S. Eskandari, and J. Clark, "Systemizing the challenges of auditing blockchain-based assets," *Journal of Information Systems*, vol. 35, no. 2, pp. 61–75, 2021.

[2] A. Posadzki, "Crypto companies struggle to find auditors willing to sign off on books," *The Globe and Mail*, March 2019.

[3] J. Dai and M. A. Vasarhelyi, "Toward blockchain-based accounting and assurance," *Journal of Information Systems*, vol. 31, no. 3, pp. 5–21, 2017.

[4] A. M. Rozario and C. Thomas, "Reengineering the audit with blockchain and smart contracts," *Journal of Emerging Technologies in Accounting*, vol. 16, no. 1, pp. 21–35, 2019.

[5] S.-F. Hsieh and G. Brennan, "Issues, risks, and challenges for auditing crypto asset transactions," *International Journal of Accounting Information Systems*, vol. 46, p. 100598, 2022.

[6] E. Boulianne and M. Fortin, "Risks and benefits of initial coin offerings: Evidence from impak finance, a regulated ico," *Accounting Perspectives*, vol. 19, no. 4, pp. 413–437, 2020.

[7] Globe and Mail, "Crypto companies struggle to find auditors amid heightened scrutiny," March 2019.

[8] C. Wagner, "As crypto auditors call it quits, what will take their place?" https://blockworks.co/news/crypto-auditors-call-it-quits, 2022.

[9] C. Ellis, T. E. Adams, and A. P. Bochner, "Autoethnography: an overview," *Historical social research/Historische sozialforschung*, pp. 273–290, 2011.

[10] C. R. Kothari, *Research methodology: methods and techniques*. New Age International, 2008.

[11] R. K. Yin, *Case study research: Design and methods*. Sage publications, 2013.

[12] M. W. Toffel, "Enhancing the practical relevance of research," *Production and Operations Management*, vol. 25, no. 9, pp. 1493–1505, 2016.

[13] D. J. Cooper and W. Morgan, "Case study research in accounting," *Accounting Horizons*, vol. 22, no. 2, pp. 159–178, 2008.

[14] G. Vinten, "Participant observation: A model for organisational investigation?" *Journal of Managerial Psychology*, vol. 9, no. 2, pp. 30–38, 1994.

[15] D. W. Allen, C. Berg, and A. M. Lane, "Why airdrop cryptocurrency tokens?" *Journal of Business Research*, vol. 163, pp. 1139–1145, 2023.

[16] R. Dunn, J. G. Jenkins, and M. D. Sheldon, "Bitcoin and blockchain: Audit implications of the killer bs," *Issues in Accounting Education*, vol. 36, no. 1, pp. 43–56, 2021.

[17] N. Webb, "A fork in the blockchain: income tax and the bitcoin/bitcoin cash hard fork," *North Carolina Journal of Law & Technology*, vol. 19, no. 4, p. 283, 2018.

[18] Ethereum Foundation, "The merge: Ethereum's transition to proof of stake," https://ethereum.org/en/upgrades/merge/, 2022.

[19] R. Ver and J. Wu., "Bitcoin cash planned network upgrade is complete," *Bitcoin Cash Blog*, 2018.

[20] Optimism Collective, "Optimism protocol," https://github.com/ethereum-optimism/optimism, 2023.

[21] N. E. Vincent and A. M. Wilkins, "Challenges when auditing cryptocurrencies," *Current Issues in Auditing*, vol. 14, no. 1, pp. A46–A58, 2020.

[22] I. Eyal, "On cryptocurrency wallet design," *3rd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2021)*, 2022.

[23] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. Li, and Y.-a. Tan, "Secure multi-party computation: theory, practice and applications," *Information Sciences*, vol. 476, pp. 357–372, 2018.

[24] BDO USA, "Service organization control (soc) reports," https://www.bdo.com/services/audit-assurance/soc-reports, 2023.

[25] A. Kroeger and A. Sarkar, "The law of one price and bitcoin arbitrage," *Liberty Street Economics*, 2017.

[26] International Financial Reporting Standards Foundation, "Ifrs 13 fair value measurement," https://www.ifrs.org/, 2011.

[27] US Department of the Treasury, "U.s. treasury sanctions notorious virtual currency mixer tornado cash," https://home.treasury.gov/news/press-releases/jy0916, 2022.

[28] I. G. A. Pernice, S. Henningsen, R. Proskalovich, M. Florian, and H. Elendner, "Monetary stabilization in cryptocurrencies: Design approaches and open questions," in *CVCBT*, 2019.

[29] C4 Security, "C4 cryptoasset security standard audit," https://github.com/cryptoconsortium/CCSS, 2023.

[30] A. Gaggioli, S. Eskandari, P. Cipresso, and E. Lozza, "The middleman is dead, long live the middleman: The "trust factor" and the psycho-social implications of blockchain," *Frontiers in Blockchain*, vol. 2, p. 20, 2019.

[31] S. Eskandari, M. Salehi, W. C. Gu, and J. Clark, "Sok: oracles from the ground truth to market manipulation," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, ser. AFT '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 127–141. [Online]. Available: https://doi.org/10.1145/3479722.3480994

[32] K. M. Bakarich, J. Castonguay, and P. E. O'Brien, "The use of blockchains to enhance sustainability reporting and assurance," *Accounting Perspectives*, vol. 19, no. 4, pp. 389–412, 2020.

[33] M. A. Vasarhelyi and F. Halper, "The continuous audit of online systems," *Auditing: A Journal of Practice and Theory*, vol. 10, pp. 110–125, 1991.

[34] Y. Wang and A. Kogan, "Designing confidentiality-preserving blockchain-based transaction processing systems," *International Journal of Accounting Information Systems*, vol. 30, pp. 1–18, 2018.

[35] J. Schmitz and G. Leoni, "Accounting and auditing at the time of blockchain technology: A research agenda," *Australian Accounting Review*, vol. 29, no. 2, pp. 331–342, 2019.

[36] C. Fisch, "Initial coin offerings (icos) to finance new ventures," *Journal of Business Venturing*, vol. 34, no. 1, pp. 1–22, 2019.

[37] H. Han, R. K. Shiwakoti, R. Jarvis, C. Mordi, and D. Botchie, "Accounting and auditing with blockchain technology and artificial intelligence: A literature review," *International Journal of Accounting Information Systems*, vol. 48, p. 100598, 2023.

[38] T. D. Bauer and C. Estep, "One team or two? investigating relationship quality between auditors and it specialists," *Contemporary Accounting Research*, vol. 36, no. 4, pp. 2142–2177, 2019.

[39] R. M. Hirsch, "The effect of it specialist knowledge and spatial distance on the audit of information technology controls," *The Accounting Review*, vol. 95, no. 3, pp. 193–217, 2020.

[40] A. Regelbrugge, "An internal auditor's guide to auditing blockchain," https://www2.deloitte.com/us/en/pages/risk/articles/internal-auditing-guide-to-blockchain.html, 2022.

[41] P. Brody, "Ey blockchain analyzer: Reconciler," https://www.ey.com/en_gl/blockchain-platforms/reconciler, 2022.

[42] Canadian Public Accountability Board, “The use of ai in the audit – balancing innovation and risk,” https://cpab-ccrc.ca/, 2024.

[43] Bank of England, “Financial stability in focus: Cryptoassets and decentralized finance,” https://www.bankofengland.co.uk/financial-stability-in-focus/2022/march-2022, 2022.

[44] KPMG, “The rise of cryptoasset adoption in canada,” https://kpmg.com/ca/en/home/insights/2022/03/the-rise-of-cryptoasset-adoptionin-canada.html, 2022.

[45] Office of the Superintendent of Financial Institutions, “Interim arrangements for the regulatory capital and liquidity treatment of cryptoasset exposures,” https://www.osfi-bsif.gc.ca/, 2022.

[46] Canadian Security Administrators, “Regulation of crypto assets,” https://www.securities-administrators.ca/, 2022.

[47] Financial Reporting and Assurance Standards Canada, “Financial reporting and assurance standards, accounting standards board’s, accounting for crypto-asset activities,” 2023.

[48] Kraken, “Proof of reserves or proof of nothing: There is no in between,” https://blog.kraken.com/, 2022.

[49] G. G. Dagher, B. Bünz, J. Bonneau, J. Clark, and D. Boneh, “Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges,” in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 720–731.

[50] J. G. Coyne and P. L. McMickle, “Can blockchains serve an accounting purpose?” *Journal of Emerging Technologies in Accounting*, vol. 14, no. 2, pp. 101–111, 2017.

[51] P. W. Abreu, M. Aparicio, and C. J. Costa, “Blockchain technology in the auditing environment,” *Paper presented at the 13th Iberian Conference on Information Systems and Technologies*, 2018.