Audit Financiar, XXIII, Nr. 1(177)/**2025**, *197-209*
ISSN on-line: 1844-8801

Navigating Auditing Risks in the Crypto Asset Landscape

Georgiana – Iulia LAZEA (TRIFA), Ph. D. Student,
West University of Timişoara, Romania,
e-mail: georgiana.lazea87@e-uvt.ro

Univ. Prof. Habil. Ovidiu – Constantin BUNGET, Ph. D.,
West University of Timişoara, Romania,
e-mail: bunget.ovidiu@e-uvt.ro

Anca-Diana BĂLAN, Ph. D.,
West University of Timişoara, Romania,
e-mail: anca.sumanaru94@e-uvt.ro

Mircea Ştefan SOLOVĂSTRU, Ph. D.,
Bucharest Stock Exchange,
e-mail: mircea_solovastru@yahoo.com

Abstract

The rise of crypto assets presents unique challenges and risks for auditors, requiring a revaluation of traditional auditing practices. This paper explores the inherent, control, valuation, and related risks associated with crypto assets, emphasising the complexities of valuation, compliance, and fraud detection. Starting from a bibliometric visualisation in VOSviewer, it points out thematic trends and key concepts in crypto auditing. The database was downloaded from the Web of Science Core Collection (2000-2024 Q3). The findings offer valuable insights for auditors, policymakers, investors, researchers, and practitioners who rely on accurate audits to make informed decisions and build trust and transparency in the crypto ecosystem.

Key words: *cryptocurrency; crypto assets; risk; audit risk; inherent risk; control risk;*

JEL Classification*: M42, G32, K34, O33*

To cite this article:
Lazea (Trifa), G.-I., Bunget, O.-C., Bălan, A.-D., Solovăstru, M. Ş. (2025), Navigating Auditing Risks in the Crypto Asset Landscape, *Audit Financiar*, vol. XXIII, no. 1(177)/2025, pp. 197-209, DOI: 10.20869/AUDITF/2025/177/006

To link this article:
http://dx.doi.org/10.20869/AUDITF/2025/177/006
Received: 20.11.2024
Revised: 21.11.2024
Accepted: 23.01.2025

Introduction

In the rapidly evolving world of digital finance, the emergence of crypto assets has brought significant opportunities and challenges for auditors.

The theme of crypto assets auditing risks is important as they become more integrated into mainstream finance, and auditors face new challenges in assessing their valuation, compliance, and fraud detection. Traditional auditing methods may not be sufficient for these decentralised and volatile assets, making it crucial to develop specialised approaches.

The purpose of this article is to review the existing scientific literature concerning the key risks auditors face when dealing with crypto asset transactions. These risks include inherent risk, control risk, valuation risk and compliance challenges. A clear understanding of these issues is essential for maintaining financial integrity, ensuring accurate reporting, and preventing illegal activities such as money laundering and terrorist financing.

This research's contribution goes beyond auditors—it is highly relevant for regulators, businesses, and investors who rely on accurate audits to make informed decisions in the increasingly digital economy. By addressing the risks involved, auditors can help build trust and transparency in the crypto ecosystem.

The study has three main objectives: first, to identify and analyse the audit risks associated with crypto asset transactions, including valuation challenges and fraud risk; second, to evaluate how blockchain technology affects the audit process by increasing transparency and security; and third, to explore how technological advancements based on blockchain can be used to mitigate crypto audit risks.

In order to meet the research goals, the authors outlined several research questions:

RQ1: What are the most significant audit risks associated with cryptocurrency transactions?

RQ2: How does using blockchain technology impact the audit process, particularly verifying transactions and detecting fraud?

RQ3: How can technological advancements, such as blockchain auditing tools, help minimise the risks associated with crypto asset audits?

Answering these questions will provide a more comprehensive understanding of the risks involved in cryptocurrency auditing while offering practical insights for auditors, regulators, and businesses.

1. Literature review

Cryptocurrencies represent a unique subset of crypto assets, which operate on decentralised networks known as blockchains (Alsalmi, Ullah, & Rafique, 2023; Makurin et al., 2023). In these networks, transaction data is recorded publicly but without revealing the identities of transacting parties. Unlike traditional assets, the absence of centralised oversight and the high volatility in cryptocurrency prices create unique challenges for auditors, complicating the identification of misstatements, fraud, or non-compliance.

Crypto assets' decentralised, often opaque nature introduces risks that traditional auditing methods may struggle to manage. As the digital asset ecosystem becomes more integrated with the conventional financial system, it introduces new risks that echo traditional finance's market failures and vulnerabilities.

A further complication is the risk of using crypto assets for money laundering and terrorist financing. With fast, globally accessible transactions and the option for anonymity, these assets are vulnerable to misuse. As such, the adequate supervision and regulation of crypto asset service providers are essential to mitigate these risks.

To effectively audit crypto assets, auditors must understand the unique characteristics and risks associated with these digital assets. This requires a deep understanding of the underlying blockchain technology, the various types of cryptoassets, and the regulatory landscape governing their use. Incorporating blockchain technology into the auditing processes (Lombardi et al., 2022) has the potential to transform audits by enhancing transparency and clarity (Bonyuet, 2020; Dai & Vasarhelyi, 2017; Abdennadher et al., 2022; Dyball & Seethamraju, 2022).

Blockchain's ability to record transactions in real-time, provide tamper-proof data, and timestamp every transaction (Buhussain & Hamdan, 2023) while keeping user information private (Pan, Vaughan, & Wright, 2023) has the potential to reshape how audits are conducted. Blockchain technology can enhance transparency and reliability, but auditors' expertise and discernment remain irreplaceable in navigating the unique complexities of crypto assets (Coyne & McMickle, 2017).

2. Research method

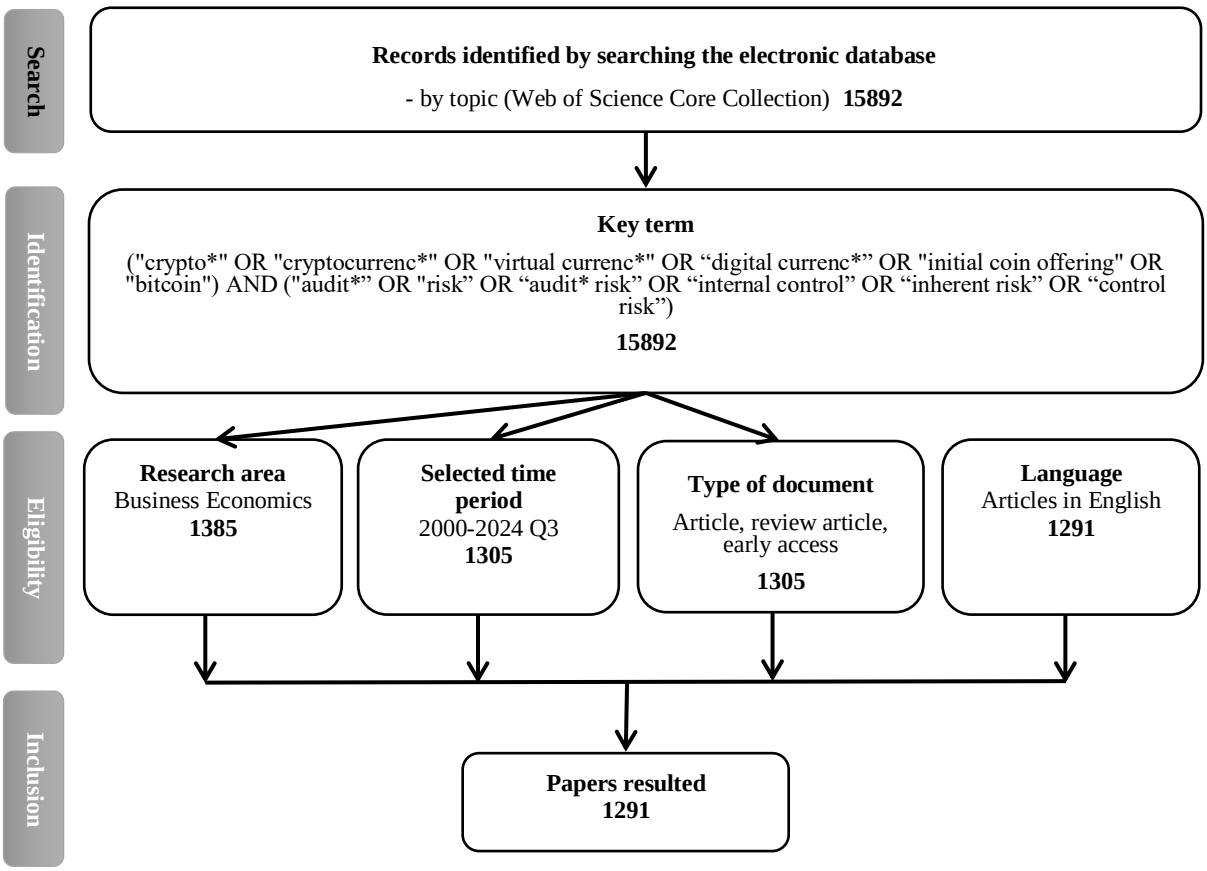
To identify pertinent literature on cryptocurrency auditing risk (CAR), the authors devised a search strategy incorporating specific keywords and utilising the Web of Science (WoS) database. This platform is an indispensable tool for researchers, providing comprehensive access to scholarly literature and ensuring high-quality peer-reviewed publications.

A customised search strategy was implemented, utilising the search string ("crypto*" OR "cryptocurrenc*" OR "virtual currenc*" OR “digital currenc*” OR "initial coin offering" OR "bitcoin") AND ("audit*" OR "risk" OR “audit* risk” OR “internal control” OR “inherent risk” OR “control risk”) to retrieve articles aligned with the research topic.

To maintain consistency and accessibility, the study included only English-language articles from various peer-reviewed sources, such as journal articles, reviews, and early-access publications. Data was gathered from the Web of Science on October 15, 2024, covering a period of rapid development in cryptocurrency and blockchain technology. Articles published between 2000 and 2024 Q3 were considered, allowing the authors to track trends and developments.

After applying specific criteria, the search returned 1291 research papers on CAR within the business economics field. *Figure no. 1* outlines the search process and the specific inclusion and exclusion criteria applied.

Figure no. 1. Flowchart of systematic selection of studies on CAR



Source: data processed by authors, 2024

The study's main objective is to identify and analyse existing research on CAR in business economics, management, accounting, and legislation.

To ensure consistency, we standardised the keywords in the database. This included merging variations of terms like "crypto/s", "cryptocurrency/ies", "cryptoasset/s", and „currency/ies". We also unified phrases such as "central bank digital currency/ies/CBDC", "decentralised finance/DEFI", „anti-money laundering/AML", „distributed ledger technology/DLT", and "blockchain technology/blockchain". After this standardisation, we analysed the research topics using keyword co-occurrence and thematic analysis.

3. Bibliometric review of the topics researched

3.1 Keyword Co-occurrence Analysis

Figure no. 2 visualises interconnected keywords related to cryptocurrency and auditing risks. Each node represents a keyword, while the connecting lines indicate how frequently these terms appear together in the analysed documents. The size of each node reflects the frequency of the keyword's occurrence, and the thickness of the lines signifies the strength of the association between them. By setting a threshold of five occurrences for each keyword, we narrowed our focus to 157 relevant terms out of 1291. VOSviewer (van Eck & Waltman, 2023) then analysed the strength of the connections between these co-occurring keywords.

The visualisation reveals the interconnections between several thematic clusters, highlighting the complex nature of crypto assets auditing risks. The connections between thematic areas emphasise the interdisciplinary nature of cryptocurrency auditing risks, incorporating aspects of economics, finance, law, and technology.

For instance, "cryptocurrency" and "blockchain" introduce *inherent risks* due to their volatility, decentralisation, and lack of traditional oversight. Keywords like "systemic risk", "portfolio optimisation", and "financial risk" reflect concerns regarding market volatility and its implications for financial statements.

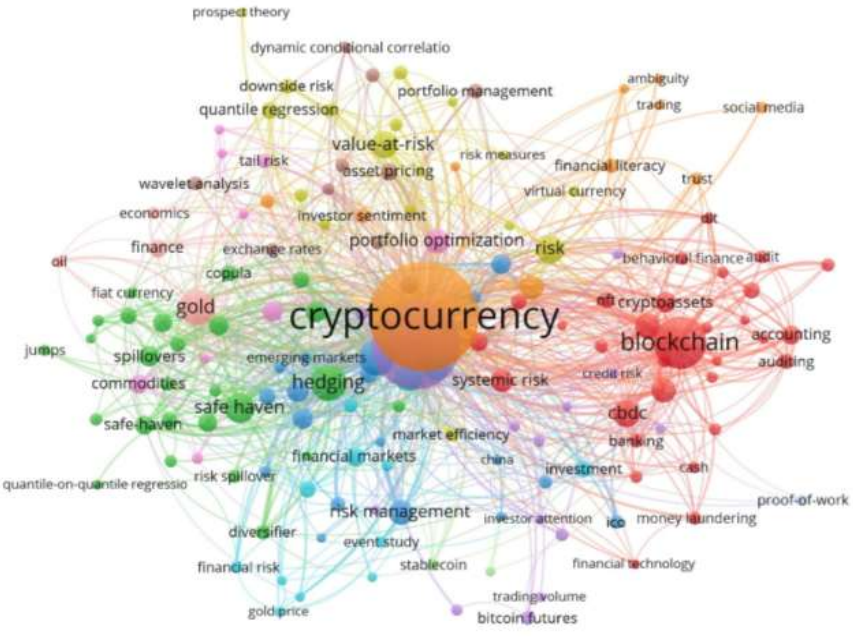
Additionally, the relationship between the "blockchain" node and terms like "auditing" and "DLT" (distributed ledger technology) suggests that auditors are using blockchain technology to improve transparency and control.

The proximity of terms such as "valuation", "price", and "volatility" near the "cryptocurrency" node suggests that accurately valuing these assets is a significant concern. Furthermore, terms like "hedging", "gold", and "value-at-risk" also point to the challenge of valuing crypto assets similarly to traditional assets like gold, but with more significant uncertainty.

Fraud risk refers to the potential for intentional misstatements, misrepresentations, or omissions in financial reporting, and the realm of cryptocurrency, this risk takes on new dimensions. The mapping of related keywords clearly illustrates the connections between "cryptocurrency", "money laundering", "trust", and "proof-of-work". This highlights how crypto transactions' decentralised and often opaque nature can foster environments where fraudulent activities can thrive.

Additionally, the map includes references to "CBDCs" (central bank digital currencies) and "financial regulation", pointing to the importance of regulatory bodies' efforts to create frameworks to monitor and control crypto transactions. *Regulatory and compliance risks* refer to the uncertainty about how regulation changes or the enforcement of existing rules could impact a business operating in the cryptocurrency space.

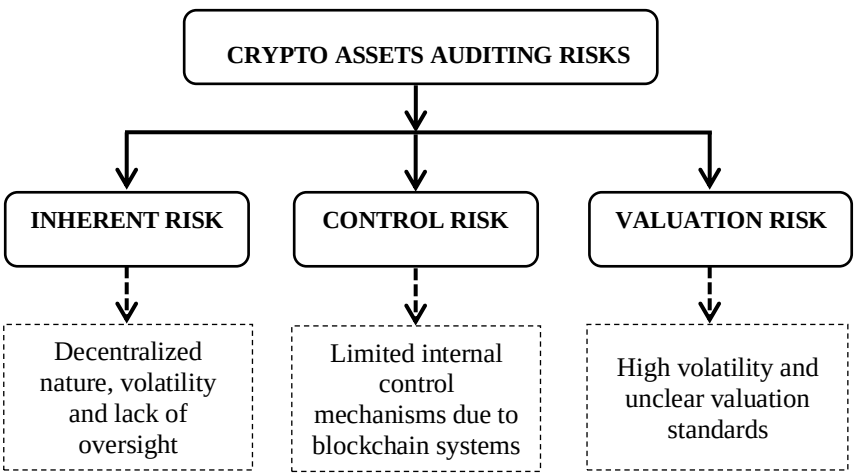
Figure no. 2. Co-occurrence of author keywords for CAR studies



Source: authors' projection, 2024

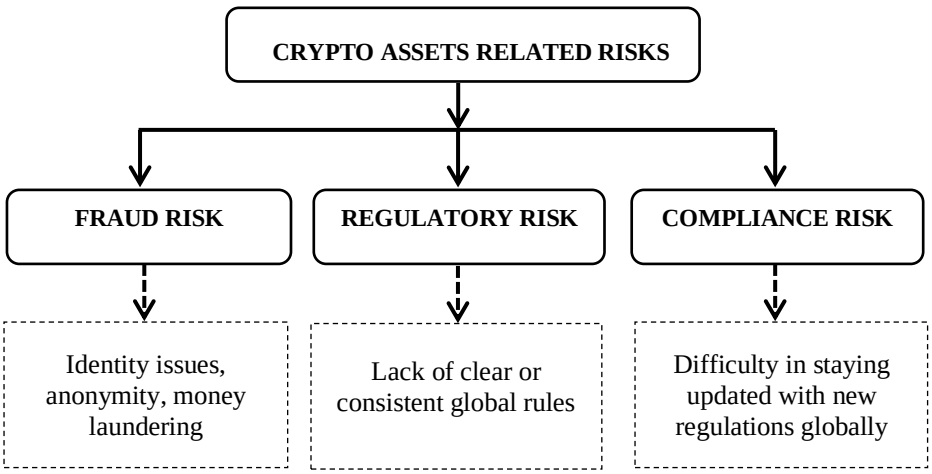
Therefore, starting from the keywords cluster, the authors can identify the three main auditing risks regarding crypto assets (***Figure no. 3***): inherent risks, control risks, valuation risks, and associated risks (***Figure no. 4***), such as fraud risk, regulatory risk, and compliance risk. These risks will be further detailed and explored in the thematic review section, providing a comprehensive overview of the challenges which auditors face in this rapidly evolving field.

Figure no. 3. Crypto assets auditing risks scheme



Source: authors' projection, 2024

Figure no. 4. Crypto assets related risks scheme



Source: authors' projection, 2024

3.2 Thematic Review of Key Auditing Risks and Challenges

It is common knowledge that audits are critical examinations of projects, combining objective analysis with subjective judgment (Kampakis, 2022) to form a final opinion. An auditor's duty is to gather credible evidence to form an opinion. This process is often hindered by difficulties verifying the completeness and accuracy of records and the reliability of the data collected (Atik & Kelten, 2021).

As more companies integrate cryptocurrency investments into their portfolios, there is a growing need for audit and advisory services specifically designed for these digital assets (Klopper & Brink, 2023; Ozeran & Gura, 2020; Smith, 2023). Auditors can utilise existing accounting standards to evaluate how companies report and manage cryptocurrency holdings, helping to ensure accuracy in financial reporting and regulatory compliance (Klopper & Brink, 2023). Yet, the emerging nature of the cryptocurrency sector poses unique challenges. Ozeran and Gura (2020) highlight that many auditors lack substantial experience in this area, raising concerns about their technological readiness to accurately identify and manage the risks associated with blockchain-based audits (Pimentel & Boulianne, 2020). Deciding whether to accept or continue auditing a company with significant cryptocurrency activity is challenging. Risks should be accurately evaluated before client acceptance and audit planning (Ozeran & Gura, 2020). Internal and external auditors should consider this issue (Rooney, Aiken, & Rooney, 2017). The lack of clear and consistent regulatory guidelines for crypto assets compounds this challenge.

It is particularly important to develop clear and effective auditing standards to ensure the integrity and transparency of metaverse transactions, given the potential risks associated with revenue recognition, security vulnerabilities, and the decentralised nature of metaverse platforms (Pandey & Gilmour, 2024).

Auditing crypto assets is complex due to their variety, platform complexity, rapid changes, market volatility, and evolving regulations. Blockchain's "proof-of-work" concept requires auditors to rely on experts to evaluate asset existence, ownership, and fair value (Ozeran & Gura, 2020). Several studies have provided detailed guidance on auditing blockchain architectures. For instance, White, King, and Holladay (2020) explored internal control and operational risks linked to private blockchains, while Liu, Wu, and Xu (2019) highlighted differences in auditing between permissioned and permissionless blockchains. These studies emphasise the importance of designing and assessing internal controls and suggest leveraging blockchain for continuous auditing (Pimentel & Boulianne, 2020).

Traditional audit procedures like confirmations, internal control assessments, document inspection, and reconciliations are used to gather evidence. For cryptocurrency transactions, auditors must specifically verify ownership of private keys and the appropriate party responsible for recording transactions (Vincent & Wilkins, 2020). During an audit, the auditor must assess the risks of material misstatement in financial reports. This involves considering information from client acceptance and previous engagements. The engagement team should discuss the entity's susceptibility to misstatements and the applicability of financial reporting standards (IAASB, 2019).

When assessing cryptoasset transaction risks, auditors should consider the materiality of such transactions. This involves calculating planning materiality and comparing cryptoasset balances to the threshold. Materiality in auditing refers to the threshold below which an error or omission is not considered significant enough to affect the economic decisions of users of the financial statements (IAASB, 2009). Determining this threshold becomes challenging in the case of cryptocurrency transactions due to the extreme volatility of the market, constantly evolving regulations and the complex nature of these digital assets. Additionally, auditors should evaluate the effectiveness of exchange controls for entities using crypto exchanges. Factors to consider include exchange ownership, reputation, location, liquidity, trading volume, and the availability of service auditor reports (Ozeran & Gura, 2020).

Risk management involves identifying, assessing, and mitigating risks that could hinder an organisation's ability to achieve its goals. This process requires understanding the organisation's risk tolerance, analysing potential fraud scenarios, and addressing technology-related risks. Furthermore, it evaluates the effectiveness of risk assessment and communication processes (Rooney, Aiken & Rooney, 2017).

Tan and Low (2019) suggest that blockchain will primarily function as a database engine, influencing various audit stages, including financial statement audits, engagement planning, risk assessment, and gathering audit evidence, as each stage interacts with the recorded data. Blockchain could improve auditors' access to client information and support continuous auditing. However, its benefits may not extend to areas requiring significant judgment, such as accounting estimates. Despite blockchain's perceived reliability, auditors should maintain a healthy level of scepticism, recognising that this technology is not immune to errors or potential fraud (Fuller & Markelevich, 2020).

Finally, the availability of higher-quality and more accessible audit evidence in many areas of the audit could shift the audit approach, freeing up more resources to focus on subjective areas (Fuller & Markelevich, 2020). These adjustments in audit focus and evidence-collection methods may help address the evolving demands of cryptoasset auditing and maintain audit integrity across digital asset transactions.

Auditors must evaluate the inherent and control risks of cryptocurrencies (Angeline et al., 2021; Dunn, Jenkins, & Sheldon, 2021; Tzagkarakis & Maurer, 2023; Sheldon, 2023).

Inherent risks exist due to the nature of the business or the environment in which it operates. In this case, the inherent risks include the vulnerability of endpoints to hacking, the risk of private key theft, and the complexity of accounting for blockchain transactions (Bonyuet, 2020). Integrating distributed ledgers and cryptography minimises the risk of data tampering or loss (Fuller & Markelevich, 2020). Another example is the valuation difficulty when holding cryptocurrencies over time, as highlighted by Smith, Petkov, and Lahijani (2019).

Evaluating inherent risks in cryptocurrency is crucial for ensuring auditors can effectively perform their engagements (Harrast, McGilsky & Sun, 2022). A key challenge for auditors working with cryptocurrency is its high price volatility (Angeline et al., 2021). These frequent price swings complicate accurate valuation, requiring both internal and external auditors to exercise significant caution in estimating cryptocurrency values and reviewing transactions (Gomaa, Gomaa, & Stampone, 2019). Auditors must carefully account for factors such as transaction dates, estimation methods, and underlying assumptions.

To address these risks, auditors have specific risk assessment procedures available for evaluating crypto assets, which include: 1) verifying balances within cryptocurrency wallets and trading accounts; 2) confirming asset ownership via third-party validation; 3) reviewing whitepapers and trading contracts; and 4) assessing internal controls related to the safeguarding of cryptocurrency holdings (Ozeran & Gura, 2020).

Assessing the completeness of cryptoassets and related transactions can be challenging due to public keys and addresses lacking transparency. The risk of inadvertently overlooking a wallet owned by the entity may affect financial statements (Ozeran & Gura, 2020). A significant risk is the loss of private keys, leading to access loss. Backup policies and segregation of duties can reduce this risk (Ozeran & Gura, 2020).

Another inherent risk is the blockchain's vulnerability to manipulation by a majority holder. This could lead to fraudulent transactions, compromised data integrity, and potential financial losses (Bonyuet, 2020). Additionally, the cryptocurrency environment may attract risk-tolerant individuals, and inexperience in this field can lower auditor confidence. Auditors with experience in cryptocurrency perceive less inherent risk, possibly due to their ability to effectively identify and weigh relevant information cues (Harrast, McGilsky & Sun, 2022).

The authors consider that relying solely on data analytics for testing is another inherent risk, as it may lead to overconfidence in the accuracy of financial statements.

To mitigate the risk of misstatements, companies would likely implement robust internal controls to prevent material errors. For cryptoassets, these controls would involve rigorous multi-stage reviews of the assumptions used in valuation (Smith, Petkov & Lahijani, 2019). Comprehensive audit procedures are essential for mitigating detection risk, and in some cases, auditors may need to engage high-cost valuation specialists. This increased scrutiny can significantly raise audit costs, impacting new and existing client engagements (Smith, Petkov & Lahijani, 2019; Bonyuet, 2020).

Control risks. Controls are procedures designed to mitigate risks and ensure an organisation achieves its operational goals, maintains accurate financial records, and adheres to legal and regulatory requirements (Rooney, Aiken & Rooney, 2017). Due to digital assets' technical complexities and security challenges, companies face unique control risks regarding cryptocurrencies. Many companies lack strong internal controls for securing digital wallets or ensuring proper accounting for cryptocurrency transactions, leaving them vulnerable to hacking or fraud.

Control risks refer to the possibility that an organisation's internal controls (Smith & Castonguay, 2020) may fail to prevent or detect issues in financial reporting. They arise from the absence or failure of internal controls to mitigate inherent risks. Examples of control risks in this context include inadequate access controls, weak cryptography features, and a lack of proper validation controls (Bonyuet, 2020). Additionally, unauthorised access to private keys – a critical security measure for cryptocurrency holdings – represents a significant control risk that could result in substantial financial misstatements if not adequately managed (Harrast, McGilsky & Sun, 2022; Gurdgiev & Fleming, 2021).

A notable control risk specific to blockchain environments is the pseudonymous nature of cryptocurrency transactions, which presents challenges in accurately recording and reporting financial transactions (Harrast, McGilsky & Sun, 2022). This highlights the need for robust internal controls, as auditors often rely on these controls to accurately assess a company's financial health (Bellucci, Cesa Bianchi & Manetti, 2022; Fuller & Markelevich, 2020; Dyball & Seethamraju, 2022; Bauer et al., 2023).

While blockchain technology is still relatively new, internal auditors must adapt their approaches to evaluate it while adhering to established professional standards. As Rooney, Aiken, and Rooney (2017) suggest, such adaptation will enable auditors to provide reliable assurance despite the unfamiliar territory of blockchain. The dependence on a blockchain system, however, introduces additional audit risks associated with the controls over the information it contains. Auditors

must carefully assess these controls to understand the audit risks related to blockchain-based financial data (Fuller & Markelevich, 2020).

To effectively assess blockchain-based systems, internal audit teams should invest in training to understand the technology and engage in the early planning stages of blockchain applications. This enables auditors to conduct real-time audits and provide timely insights, enhancing their value to organisations. Standards bodies should also develop guidelines to ensure blockchain applications meet governance principles and deliver the promised value. Internal auditors' deep understanding of the business context is essential for effectively assessing governance, risk, and control environments.

Challenges in adopting blockchain include issues related to scalability, flexibility, and compliance with statutory requirements, which can impact audit effectiveness. Auditors relying on blockchain systems must ensure these systems incorporate strong access and validation controls to mitigate the risk of undetected errors or fraud (Bonyuet, 2020). With real-time transaction visibility, blockchain-based applications can enable auditors to conduct continuous audits and provide timely insights. For this to be effective, internal audit teams should invest in training to understand blockchain technology thoroughly.

Internal audits have been shown to reduce organisational risk and improve performance. Carcello et al. (2020) found that internal audits are associated with lower perceived risk and higher performance ratings, enhancing operational effectiveness. This insight further underscores the importance of comprehensive audit procedures, especially as companies integrate blockchain applications.

Therefore, to provide accurate and reliable assurance on the effectiveness of governance, risk management, and internal controls in blockchain environments, internal auditors must have a comprehensive understanding of blockchain technology and its applications (Rooney, Aiken & Rooney, 2017).

Valuation risks. Valuing cryptocurrencies presents significant challenges due to their speculative nature, extreme price fluctuations (Tzagkarakis and Maurer, 2023), and lack of standardised accounting treatment. The accurate valuation of cryptoassets is a significant challenge, which makes consistent application of fair value accounting difficult.

Both companies and their external auditors struggle to value these assets accurately. Additionally, verifying the existence and completeness of these assets can be complex due to the subjective nature of the information, making valuation and asset verification highly risky for auditors (Smith, Petkov & Lahijani, 2019).

Fraud risks. Cryptocurrencies' pseudonymous nature creates a potential for fraud, such as asset misappropriation, transaction manipulation, money laundering and illicit financing. This anonymity allows for behaviours like underreporting income, which can complicate audit and compliance efforts.

However, blockchain's transparent ledger allows stakeholders to independently verify and audit financial transactions, reducing the risk of fraud, manipulation, or misrepresentation. This transparency also promotes participant accountability (Proelss, Schweizer & Sevigny, 2024).

As noted by Bennett et al. (2020), the use of smart contracts further supports transparency in crypto trading. Real-time data from blockchain technology enables more timely reporting and assurance, allowing accountants and auditors to monitor fraud risks and evaluate IT controls effectively.

Regulatory and compliance risks. The evolving regulatory landscape for cryptocurrencies poses significant compliance challenges. Therefore, companies may unintentionally fail to meet tax or accounting regulations, exposing them to legal and audit risks. Despite regulatory efforts, cryptocurrency transactions' global and pseudonymous nature complicates enforcement, as cross-border exchanges and anonymous transactions hinder individuals' or companies' tracking (Harrast, McGilsky & Sun, 2022).

Audit standard setters face difficulties keeping pace with cryptocurrencies' rapid technological advancements. Traditional, lengthy processes for updating audit standards are ill-suited for such fast-evolving technologies. To maintain public trust, standards must adapt quickly to match the speed at which entities adopt and implement these new technologies (Bennett et al., 2020).

Table no. 1 summarises the challenges regarding crypto asset transactions, the risk category, and the risk mitigation strategy that should be considered when planning and conducting an audit.

Table no. 1. Risk mitigation strategies for crypto assets – Auditor perspective

	Challenges	Risks	Risk Mitigation Strategy
Auditing risks	Vulnerability to transaction manipulation	Inherent risk	Auditor involvement in transaction validation (Bonyuet, 2020).
	Misappropriation of assets and fraudulent misreporting		Blockchain offers excellent immunity to data security risks because modifying all copies simultaneously would be impossible (Fuller & Markelevich, 2020).
	Absence of mechanisms to track transactions in multiple ledgers		Develop an appropriate mechanism to track transactions.
	Difficulty in determining the crypto value		Research and apply appropriate valuation methods for cryptocurrencies, considering market capitalisation, trading volume, and underlying technology.
	Unauthorised private key access		Identifying who controls the keys and the minimum number of users needed to authorise a transaction (Harrast, McGilsky & Sun, 2022).
	Unsecured private key		Understanding cryptocurrency exchange interactions and balance verification (AICPA, 2024).
	Unaccounted crypto wallet		Implement robust security measures such as multi-factor authentication and regular security audits.
	Unidentified related-party transaction		Ensure that clients disclose relevant information about cryptocurrency transactions.
	Misrepresentation of ownership		Implement robust Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures to verify users' identities and prevent fraud (Lazea, Bunget & Lungu, 2024).
	Lost private key		Educate clients about the importance of proper key management and backup practices, including backup policies and segregation of duties (Ozeran & Gura, 2020).
	Crypto sent to the wrong address		Educate clients about verifying recipient addresses and the potential consequences of errors.
	Lack of flexibility and error correction	Control risk	Correcting an error requires adding a new entry to the blockchain, which other users must validate. Add a new block to indicate that the old data is incorrect and has been replaced (Abdennadher et al., 2022).
	Heavy signature verification for transactions		Consensus process to validate and add transactions to the ledger (Abdennadher et al., 2022).
	Evaluate blockchain as a ledger		Determine its reliability and relevance and verify the entity's ownership of wallet addresses (Alhasana & Alrowwad, 2022).
	Identify potential fraud		Develop double-booking balances or provide wallet addresses to multiple auditors (Alhasana & Alrowwad, 2022).
	Assess custody		Determine whether the entity has exclusive control of the digital assets or relies on third-party providers, considering cybersecurity risks (Alhasana & Alrowwad, 2022).
	Fluctuation in cryptocurrency value	Valuation risk	Introduce real-time valuation techniques and use stablecoins or other hedging instruments to minimise volatility.
	Lack of established valuation models		Develop standardised valuation models for digital assets.
Related risks	Risky crypto trading	Fraud risk	Introducing smart contracts (Bennett et al., 2020).
	Money laundering		Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations to help identify and track illicit transactions (Lazea, Bunget & Lungu, 2024).
	Regulatory changes	Regulatory and compliance risk	More certain and unified regulations.
	GDPR protects consumer data		The current focus is resolving the conflict between GDPR and blockchain technology (Arnold, 2018).

Source: authors' projection, 2024

Conclusion

The metaverse has profound implications for the future of auditing. As this technology evolves, auditors must adapt their approaches to address the unique challenges and opportunities it presents. This includes rethinking audit planning, evidence gathering, and risk assessment to fit the metaverse landscape (Pandey & Gilmour, 2024).

One of the core questions auditors face is *RQ1: What are the most significant audit risks associated with crypto assets and cryptocurrency transactions?* While blockchain offers various potential benefits, auditors must carefully evaluate the inherent, control and valuation risks linked with its adoption. A balanced approach that combines traditional audit techniques with modern data analytics while addressing security and validation concerns is essential to ensure the reliability of financial reporting.

Another crucial consideration is *RQ2: How does using blockchain technology impact the audit process, particularly verifying transactions and detecting fraud?* To address this problem, blockchain technology significantly impacts the audit process by enhancing transaction transparency, traceability, and reliability. One of the most notable advantages of blockchain is its decentralised nature, which allows all participants in the network to access the exact version of the transaction ledger. In terms of fraud detection, blockchain technology facilitates a more proactive approach. With its ability to track assets through every transaction step, auditors can identify anomalies or irregular patterns that may indicate fraudulent activity.

Moreover, smart contracts can automate certain audit procedures, such as compliance checks and validation. This automation not only increases efficiency but also reduces the risk of human error, which can lead to oversight in detecting fraudulent transactions.

A third pivotal inquiry is *RQ3: How can technological advancements, such as blockchain auditing tools, help minimise the risks associated with crypto asset audits?* To harness these opportunities, auditors should engage in the development of new standards and actively participate in the evolution of blockchain technology. This involves suggesting appropriate audit modules, enhancing their technical skills, and utilising artificial intelligence to boost efficiency.

Key objectives for auditors include verifying digital signatures, designing effective audit strategies, collaborating with regulatory bodies, and ensuring adequate cyber and software auditing.

In summary, auditing crypto assets is challenging due to unique risks, control issues, valuation complexities, and rapidly advancing technology. Continued research into these obstacles and creating a solid auditing framework for this type of asset are essential to maintaining accurate and dependable financial reporting in this evolving field.

Bibliography

1. Abdennadher, S. et al. (2022) The effects of blockchain technology on the accounting and assurance profession in the UAE: an exploratory study, *Journal of Financial Reporting and Accounting*. Available at: https://doi.org/10.1108/JFRA-05-2020-0151.
2. AICPA, A.I. of C.P.A. (2024) Accounting for and auditing of digital assets. Available at: https://www.aicpa-cima.com/resources/download/accounting-for-and-auditing-of-digital-assets-practice-aid-pdf.
3. Alhasana, K.A.H. and Alrowwad, A.M.M. (2022) National Standards of Accounting and Reporting in the Era of Digitalization of the Economy, *Financial and credit activity problems of theory and practice*. 1(42): 154-161, Available at: https://doi.org/10.55643/fcaptp.1.42.2022.3727.
4. Alsalmi, N., Ullah, S. and Rafique, M. (2023) Accounting for digital currencies, *Research in International Business and Finance*. Elsevier Ltd. Available at: https://doi.org/10.1016/j.ribaf.2023.101897.
5. Angeline, Y.K.H. et al. (2021) Accounting Treatments for Cryptocurrencies in Malaysia: The Hierarchical Component Model Approach, *Asian Journal of Business and Accounting*. 14(2), pp. 137-171, Available at: https://doi.org/10.22452/ajba.vol14no2.5.
6. Arnold, A. (2018) Can Blockchain Help Brands Become GDPR Compliant?, *Forbes*, December,

Available at: https://www.forbes.com/sites/andrewarnold/2018/11/20/can-blockchain-help-brands-become-gdpr-compliant/.

7. Atik, A. and Kelten, G.S. (2021) Blockchain Technology and Its Potential Effects on Accounting: A Systematic Literature Review, *Istanbul Business Research*. October, Available at: https://doi.org/10.26650/ibr.2021.50.806870.
8. Bauer, T.D. et al. (2024) Cataloging the Marketplace of Assurance Services, *Auditing: A Journal of Practice & Theory*, 43(3): 49-75, Available at: https://doi.org/10.2308/AJPT-2022-196.
9. Bellucci, M., Cesa Bianchi, D. and Manetti, G. (2022) Blockchain in accounting practice and research: systematic literature review, *Meditari Accountancy Research*. 30(7):121-146, Available at: https://doi.org/10.1108/MEDAR-10-2021-1477.
10. Bennett, S. et al. (2020) Blockchain and Cryptoassets: Insights from Practice, *Accounting Perspectives*. 19(4), Available at: https://doi.org/10.1111/1911-3838.12238.
11. Bonyuet, D. (2020) Overview and Impact of Blockchain on Auditing, *International Journal of Digital Accounting Research*. Vol. 20, pp. 31-43, Available at: https://doi.org/10.4192/1577-8517-v20_2.
12. Buhussain, G. and Hamdan, A. (2023) Blockchain Technology and Audit Profession, în: *Emerging Trends and Innovation in Business and Finance*, Available at: https://doi.org/10.1007/978-981-99-6101-6_52.
13. Carcello, J.V. et al. (2020) Are Internal Audits Associated with Reductions in Perceived Risk?, *Auditing: A Journal of Practice & Theory*, 39(3), pp. 55-73, Available at: https://doi.org/10.2308/ajpt-19-036.
14. Coyne, J.G. and McMickle, P.L. (2017) Can Blockchains Serve an Accounting Purpose?, *Journal of Emerging Technologies in Accounting*. 14(2), Available at: https://doi.org/10.2308/jeta-51910.
15. Dai, J. and Vasarhelyi, M.A. (2017) Toward Blockchain-Based Accounting and Assurance, *Journal of Information Systems*. 31(3), Available at: https://doi.org/10.2308/isys-51804.
16. Dunn, R.T., Jenkins, J.G. and Sheldon, M.D. (2021) Bitcoin and Blockchain: Audit Implications of the Killer Bs, *Issues in Accounting Education*, 36(1), pp. 43-56. Available at: https://doi.org/10.2308/ISSUES-19-049.
17. Dyball, M.C. and Seethamraju, R. (2021) Client use of blockchain technology: exploring its (potential) impact on financial statement audits of Australian accounting firms, *Accounting, Auditing and Accountability Journal*. October, vol. 35(7), pp: 1656-1684, Available at: https://doi.org/10.1108/AAAJ-07-2020-4681.
18. Fuller, S.H. and Markelevich, A. (2020) Should accountants care about blockchain?, *Journal of Corporate Accounting and Finance*. September, Available at: https://doi.org/10.1002/jcaf.22424.
19. Gomaa, A.A., Gomaa, M.I. and Stampone, A. (2019) A transaction on the blockchain: An AIS perspective, intro case to explain transactions on the ERP and the role of the internal and external auditor, *Journal of Emerging Technologies in Accounting*. 16(1), Available at: https://doi.org/10.2308/jeta-52412.
20. Gurdgiev, C. and Fleming, A. (2021) Informational efficiency and cybersecurity: Systemic threats to blockchain applications, in "Innovations in Social Finance". *Springer*, pp: 347-372, Available at: https://doi.org/10.1007/978-3-030-72535-8_16.
21. Harrast, S.A., McGilsky, D. and Sun, Y. (2022) Determining the Inherent Risks of Cryptocurrency: A Survey Analysis, *Current Issues in Auditing*. 16 (2): A10–A17, Available at: https://doi.org/10.2308/CIIA-2020-038.
22. IAASB, I.A. and A.S.B. (2009) ISA 320 materiality in planning and performing an audit.
23. IAASB, I.A. and A.S.B. (2019) ISA 315 identifying and assessing the risks of material misstatement.
24. Kampakis, S. (2022) Auditing Tokenomics: A Case Study and Lessons from Auditing a Stablecoin Project, *Journal of The British Blockchain Association*. April, vol. 5, no. 2, Available at: https://doi.org/10.31585/jbba-5-2-(1)2022.
25. Klopper, N. and Brink, S.M. (2023) Determining the Appropriate Accounting Treatment of Cryptocurrencies Based on Accounting Theory, *Journal of Risk and Financial Management*. 16(9):379, Available at: https://doi.org/10.3390/jrfm16090379.
26. Lazea, G.-I., Bunget, O.-C. and Lungu, C. (2024) Cryptocurrencies' Impact on Accounting: Bibliometric

Review, *Risks*, 12(6), pp. 94. Available at: https://doi.org/10.3390/risks12060094.

27. Liu, M., Wu, K. and Xu, J.J. (2019) How Will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain, *Current Issues in Auditing*, 13(2), pp. A19-A29. Available at: https://doi.org/10.2308/ciia-52540.
28. Lombardi, R. et al. (2022) The disruption of blockchain in auditing – a systematic literature review and an agenda for future research, *Accounting, Auditing and Accountability Journal*. 35(7):1534-1565, Available at: https://doi.org/10.1108/AAAJ-10-2020-4992.
29. Makurin, A. et al. (2023) Management of Cryptocurrency Transactions from Accounting Aspects, *Economics ecology socium*. 7(3): 26-35, Available at: https://doi.org/10.31520/2616-7107/2023.7.3-3.
30. Ozeran, A. and Gura, N. (2020) Audit and accounting considerations on cryptoassets and related transactions, *Economic Annals-XXI*. 184 (7-8), 124-132. Available at: https://doi.org/10.21003/ea.V184-11.
31. Pan, L., Vaughan, O. and Wright, C.S. (2023) A Private and Efficient Triple-Entry Accounting Protocol on Bitcoin, *Journal of Risk and Financial Management*. 16(9):400, Available at: https://doi.org/10.3390/jrfm16090400.
32. Pandey, D. and Gilmour, P. (2024) Accounting meets metaverse: navigating the intersection between the real and virtual worlds, *Journal of Financial Reporting and Accounting*. 22(2):211-226 Available at: https://doi.org/10.1108/JFRA-03-2023-0157.
33. Pimentel, E. and Boulianne, E. (2020) Blockchain in Accounting Research and Practice: Current Trends and Future Opportunities, *Accounting Perspectives*. 19(4), 325-361. Available at: https://doi.org/10.1111/1911-3838.12239.
34. Proelss, J., Schweizer, D. and Sevigny, S. (2024) Is Bitcoin ESG-Compliant? A sober look, *European Financial Management*. Vol. 30, no. 2, pp. 680-726. Available at: https://doi.org/10.1111/eufm.12451.
35. Rooney, H., Aiken, B. and Rooney, M. (2017) Q&A. Is Internal Audit Ready for Blockchain?. *Technology Innovation Management Review*. 7(10):41-44. Available at: https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_October2017.pdf.
36. Sheldon, M.D. (2023) Preparing Auditors to Evaluate Blockchains Used to Track Tangible Assets, *Current Issues in Auditing*. 18(2): 1-22. Available at: https://doi.org/10.2308/CIIA-2023-014.
37. Smith, S.S. (2023) The cryptoasset auditing and accounting landscape, in: "The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges". *Emerald Publishing Ltd*. January, pp. 13-24, Available at: https://doi.org/10.1108/978-1-80455-320-620221002.
38. Smith, S.S. and Castonguay, J.J. (2020) Blockchain and Accounting Governance: Emerging Issues and Considerations for Accounting and Assurance Professionals, *Journal of Emerging Technologies in Accounting*. November, Available at: https://doi.org/10.2308/jeta-52686.
39. Smith, S.S., Petkov, R. and Lahijani, R. (2019) Blockchain and Cryptocurrencies – Considerations for Treatment and Reporting for Financial Services Professionals, *International Journal of Digital Accounting Research*. Available at: https://doi.org/10.4192/1577-8517-v19_3.
40. Tan, B.S. and Low, K.Y. (2019) Blockchain as the Database Engine in the Accounting System, *Australian Accounting Review*, 29(2), pp. 312-318. Available at: https://doi.org/10.1111/auar.12278.
41. Tzagkarakis, G. and Maurer, F. (2023) Horizon-Adaptive Extreme Risk Quantification for Cryptocurrency Assets, *Computational Economics*. 62(3):1-36, Available at: https://doi.org/10.1007/s10614-022-10300-3.
42. van Eck, Nees Jan, and Waltman, L. (2023) VOSviewer Manual. Available at: https://www. vosviewer. com/documentation/Manual_ VOSviewer_ 1.6.20.pdf (accessed on October 31, 2024).
43. Vincent, N.E. and Wilkins, A.M. (2020) Challenges when Auditing Cryptocurrencies, *Current Issues in Auditing*, 14(1), pp. A46-A58. Available at: https://doi.org/10.2308/ciia-52675.
44. White, B.S., King, C.G. and Holladay, J. (2020) Blockchain security risk assessment and the auditor, *Journal of Corporate Accounting & Finance*, 31(2), pp. 47-53. Available at: https://doi.org/10.1002/jcaf.22433.