frontiers | Frontiers in Blockchain

TYPE Mini Review
PUBLISHED 25 April 2025
DOI 10.3389/fbloc.2025.1549729

OPEN ACCESS

EDITED BY
Marcelle Michelle Georgina Maria Von Wendland,
Bancstreet Capital Partners Ltd., United Kingdom

REVIEWED BY
Hebatallah Badawy,
Egypt-Japan University of Science and Technology, Egypt

*CORRESPONDENCE
Yunfan Zhang,
644410376@qq.com
Zifei Ma,
1220019442@student.must.edu.mo
Jiaming Meng,
1220009142@student.must.edu.mo

RECEIVED 21 December 2024
ACCEPTED 16 April 2025
PUBLISHED 25 April 2025

CITATION
Zhang Y, Ma Z and Meng J (2025) Auditing in the blockchain: a literature review.
Front. Blockchain 8:1549729.
doi: 10.3389/fbloc.2025.1549729

Auditing in the blockchain: a literature review

Yunfan Zhang*, Zifei Ma* and Jiaming Meng*

Department of Decision Sciences, School of Business, Macao University of Science and Technology, Taipa, Macao SAR, China

This investigation evaluates blockchain's dichotomous effects on auditing through systematic literature synthesis and comparative case studies of Big Four accounting firms. Empirical evidence demonstrates that distributed ledger technology enhances audit efficacy through automated transaction authentication (exemplified by PwC's 90% temporal reduction in reconciliation protocols) and machine learning-powered anomaly detection algorithms, enabling comprehensive audit sampling and continuous monitoring capabilities. Persistent technical risks remain, notably 51% consensus vulnerabilities, self-executing contract exposures, and throughput constraints in decentralized architectures, which collectively compromise system integrity. Furthermore, regulatory lacunae in cross-jurisdictional compliance frameworks and practitioners' competency deficits in cryptographic validation techniques substantially impede technological assimilation. The analysis substantiates three critical imperatives: (1) harmonized regulatory frameworks with Turing-complete compliance protocols, (2) cross-disciplinary human capital development initiatives, and (3) applied research on heterogeneous system interoperability. Strategic mitigation of these implementation barriers could transition auditing toward cryptographic trust ecosystems, contingent upon synergistic collaboration between regulatory bodies establishing adaptive governance models, corporate entities developing hybrid audit architectures, and academic institutions advancing validation methodologies.

KEYWORDS

blockchain, audit, risk management, smart contracts, regulatory compliance

1 Introduction

With the advent of big data, blockchain technology has emerged due to advancements in computing power, offering a new option in science and technology. Supported by national policies, blockchain technology has been widely applied in areas such as finance, food safety, trade, and government affairs, bringing convenience and efficiency to various sectors of society. Since ancient times, auditing has been crucial in supervising and evaluating authenticity, legitimacy, and financial information. However, with the rise of economic globalization and information fragmentation, traditional audit models face numerous challenges, such as unreliable evidence, difficulty obtaining evidence, high audit costs, and low audit efficiency. Technological innovation is one of the key solutions to these issues, as it can optimize audit processes and improve audit quality and efficiency. Blockchain technology, with its characteristics of decentralization, transparency, immutability, and traceability, provides new approaches and methods for audit work. Its application can significantly improve the authenticity and reliability of audit data, accelerate evidence collection, facilitate data sharing, reduce audit costs, and help establish a

new trust system within the audit industry. Despite its advantages like data integrity and transparency, blockchain-based auditing brings challenges, such as the need to reconstruct the credit mechanism and high technical barriers.

In summary, blockchain technology presents both opportunities and challenges. This paper explores the risks and practical impacts of blockchain auditing by analyzing its applications and associated challenges. The goal is to provide theoretical support and valuable insights for implementing the "blockchain + audit" model.

2 Methods

2.1 Literature research method

Through a systematic review of academic literature, industry reports, and trade-related materials, an in-depth analysis and summary were conducted on the limitations of blockchain technology, its application approaches in auditing, and the risks and challenges it encounters. Academic papers such as "Blockchain Audit" by Karajovic et al. (2019) and Rozario and Thomas (2019), along with other authoritative materials, have been thoroughly examined.

2.2 Case analysis method

This paper analyzes multiple application cases of PricewaterhouseCoopers (PwC) in blockchain auditing. These include launching blockchain auditing services, developing Halo tools, and cooperating with VeChain to improve supply chain transparency and achieve real-time auditing. In addition, companies such as Microsoft, KPMG, EY, and others have implemented blockchain audit practices. These specific cases illustrate the practical application of blockchain technology in the audit industry.

3 Some key blockchain audit technology

Technical encryption in the blockchain context is bifurcated into symmetric and asymmetric encryption. In symmetric encryption, compromising a single party's key jeopardizes the security of the encrypted data. Asymmetric encryption, relying on public-private key algorithms, is more intricate and slower in encryption and decryption processes (Nakamoto, 2008; Zheng, Xie, Dai, Chen and Wang, 2019). Nakamoto's pioneering work introduced the fundamental cryptographic concepts in blockchain, and Zheng et al. further explored modern encryption applications within the blockchain ecosystem.

Identity and access management (IAM) in blockchain systems empowers individuals or organizations to access appropriate resources at the right time for legitimate purposes. At the onset of IAM implementation in blockchain platforms, it is crucial to establish rigorous access policies. These policies delineate who can manage the platform and define management privileges, thereby ensuring compliance and preventing unauthorized access (Sabett, 2020; Wang, Zhang and Yang, 2021). Sabett's research focused on IAM best - practices in blockchain, and Wang et al. delved into IAM mechanisms for enhanced security.

Innovative contract technology in blockchain presents two primary risks (Buterin, 2013; Christidis and Devetsikiotis, 2016). Attackers may deploy malware or create phishing websites to pilfer user data. Additionally, smart contracts can have inherent design flaws. For instance, the 2018 Ethereum multi-signature issue immobilized over $150 million in assets. The self-executing nature of smart contracts, which minimizes human intervention, makes it difficult to rectify on-chain vulnerabilities (Luu, Chu, Olickel, Saxena and Hobor, 2016; Gramoli and Kuznetsov, 2018). Vitalik Buterin's introduction of Ethereum laid the groundwork for smart contracts, and Christidis et al. analyzed their potential risks and applications.

Figure 1 indicates the audit blockchain process.

4 Blockchain audit risks

Audit risks include inherent risks, control risks and detection risks (Arens, Elder and Beasley, 2012; Messier, Glover and Prawitt, 2017), while the application risks of blockchain auditing include security risks and technical risks (Atzei, Bartoletti and Cimoli, 2017; Zheng, Xie, Dai, Chen and Wang, 2019).

With the development of computer hardware, blockchain is vulnerable to 51% computing power attacks (Eyal and Sirer, 2014; Gervais, Karame, Wüst, Glykantzis, Ritzdorf and Capkun, 2016). Secondly, external auditors must obtain the system's public and specific private keys after blockchain-assisted auditing before accessing relevant data. Such behaviour will inevitably breed new security issues (Sabett, 2020; Yli-Huumo, Ko, Choi, Park and Smolander, 2016).

Traditional auditing relies on the endorsement of authoritative institutions, while blockchain technology turns to algorithms and smart contracts, which will trigger a new credit mechanism reconstruction (Nakamoto, 2008; Buterin, 2013). In reality, it is necessary to identify the authenticity of data, ensure data privacy and balance sharing, establish incentive mechanisms, solve related interest distribution, and reduce the cost of obtaining information (Christidis and Devetsikiotis, 2016; Zyskind and Nathan, 2015; Tapscott and Tapscott, 2016; Swan, 2015).

Blockchain auditing will likely reduce the demand for traditional auditors and impose higher-level skill requirements on them (Low, Cao and Wang, 2020; Zhao, Liu and Zhang, 2021). Auditors are now expected to have a solid understanding of basic auditing knowledge and master computer skills, possess in-depth blockchain knowledge, and demonstrate strong analysis and decision-making capabilities. However, as of now, most auditors lack exposure to blockchain-related content (Low et al., 2020).

Regarding the regulatory environment, the regulatory framework for blockchain technology is still developing in mainland China. While there are existing relevant filing regulations, the regulatory regime tailored explicitly for blockchain-based auditing remains underdeveloped (Sun, 2022; Li and Wang, 2023). Since auditing is a highly regulated activity with substantial legal, policy-oriented, and normative characteristics, the

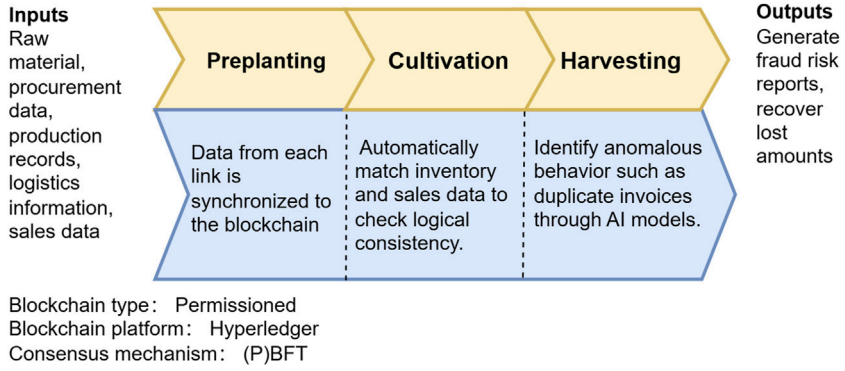

FIGURE 1
Blockchain-based data flow for supply chain auditing.

TABLE 1 Comparison of traditional audit and blockchain audit.

Aspect	Traditional audit	Blockchain audit
Data Integrity	Relies on third-party verification and manual reconciliation	Ensures data immutability and transparency through distributed ledger technology (DLT)
Audit Scope	Sampling-based approach, limited transaction coverage	Full population audit with real-time transaction verification
Evidence Collection	Requires extensive documentation and third-party confirmations	Transactions are cryptographically verified and stored on-chain
Verification Method	Based on external confirmations and internal control testing	Utilizes cryptographic proof and consensus mechanisms
Fraud Detection	Post-factum analysis with reliance on forensic investigations	Automated anomaly detection using AI-integrated blockchain platforms
Audit Efficiency	Time-consuming, labor-intensive, and subject to human error	Reduces manual workload and enables continuous auditing
Security Risks	Prone to data manipulation, unauthorized access, and fraud	Vulnerable to 51% attacks, smart contract exploits, and key mismanagement
Regulatory Compliance	Operates within well-defined legal frameworks	Regulatory uncertainty due to evolving legal frameworks for blockchain applications
Cost Structure	High due to extensive human intervention and document handling	Potentially lower due to automation and real-time verification
Role of Auditors	Auditors act as intermediaries for financial verification	Shift towards smart contract auditing and blockchain protocol assessment
Implementation Barriers	Established methodologies and infrastructure	Requires specialized technical knowledge and regulatory adaptation

absence of a comprehensive regulatory system for blockchain auditing poses potential risks to auditors.

Regarding the new risks blockchain technology brings to auditors, the complexity of blockchain systems means that auditors may face challenges in understanding and verifying the integrity of transactions. For example, the immutability of blockchain records, while a key feature, can be a double-edged sword. Suppose an error or malicious entry is made on the blockchain. In that case, it becomes challenging to correct, leading to potential misstatements in financial reporting that auditors may struggle to identify and rectify (Atzei, Bartoletti and Cimoli, 2017). Also, the security risks, such as 51% computing power attacks (Eyal and Sirer, 2014), can undermine the reliability of the blockchain-based data that auditors rely on, creating significant risks in the audit process.

Table 1 indicates ample comparisons between the traditional audit and blockchain.

5 Blockchain audit applications

5.1 Technical integration and tool innovation

5.1.1 PricewaterhouseCoopers (PwC): intelligent audit platform and AI synergy

PwC has pioneered the construction of a blockchain-based "networked audit system," which connects with enterprise financial systems in real-time through distributed ledger technology (DLT) to achieve cross-agency data sharing. For example, in a supply chain audit, the data of suppliers, logistics parties, and customers is synchronized to the blockchain, and auditors can directly verify the authenticity and integrity of transactions, reducing the manual reconciliation time by 90% in the traditional model (PWC, 2017). In addition, PwC integrates AI models, such as DeepSeek-R1, into the blockchain audit platform to automatically identify abnormal transaction patterns. In the audit case of a multinational group in 2023, the system successfully flagged five

fictitious cross-border transactions involving US$12 million, highlighting the synergistic effect of "blockchain + AI" in risk early warning. PricewaterhouseCoopers.

5.1.2 Ernst and Young (EY): zero-knowledge proofs and privacy

EY has developed the "EY Blockchain Analyzer" tool to support pass-through audits of cryptocurrencies and smart contracts. Its core innovation lies in introducing zero-knowledge proof (ZKP) technology, which allows companies to prove transaction compliance to auditors without revealing sensitive data. For example, when auditing a financial institution's crypto assets, EY verified the authenticity of its Bitcoin reserves through ZKP while protecting customer privacy (EY, 2023). This technological breakthrough solves the contradiction between blockchain transparency and enterprise data confidentiality.

5.1.3 Deloitte: private chain solutions for the financial industry

Deloitte focuses on blockchain audits in the financial sector. It has partnered with JPMorgan Chase to develop Deloitte ChainFinance, a private blockchain platform for automating processing letters of credit and trade finance. The platform uploads data such as loan origination and repayment records on-chain in real time, and auditors can automatically verify business compliance through smart contracts. According to the case data, the LC audit cycle of a bank was shortened from 14 days to 2 days, and the error rate was reduced by 75% (Deloitte, 2021).

5.1.4 KPMG: transparency in supply chain audits

KPMG designed an innovative contract-based supply chain tracking system for a blockchain audit for the retail industry. For example, when serving a global FMCG brand, the system uploads all the data of raw material procurement, production, and logistics to the chain and automatically matches inventory and sales data. Through on-chain data traceability, the audit team found fraudulent behaviour of a supplier for repeated invoicing, recovering about US$8 million in losses for the company (KPMG, 2017).

5.2 Profound impact on audit business models

5.2.1 Exponential improvement in audit efficiency

Full sample coverage replaces sample audit: Traditional audit is limited by the cost of only 5%–10% of transactions, while blockchain supports complete data analysis. Ernst and Young statistics show that its blockchain tools have increased risk coverage from 78% to 99% (EY White Paper, 2023).

Real-time audit shortening cycles: PwC's case shows that blockchain has reduced the audit cycle of a multinational company's annual report from 3 months to 6 weeks, reducing labour costs by 40% (PWC, 2017).

5.2.2 Structural changes in the audit paradigm

From "post-event verification" to "continuous monitoring," the four major firms have deployed blockchain nodes to monitor real-time transaction data in the corporate financial system. For example, Deloitte's "Smart Audit" module automatically triggers an immediate review of abnormal cash flows, such as a single transaction exceeding a threshold, shifting risk management from "correcting after the fact" to "intercepting during the event."

Audit focus shifts to smart contract logic: Since the blockchain guarantees the authenticity of data, audit resources are more invested in smart contract code auditing. KPMG has set up a dedicated "blockchain protocol review team" and found 32 contract vulnerabilities in 2023, including logical errors that could lead to duplicate payments (KPMG, 2017).

6 Limitations

While blockchain offers various benefits, its adoption in auditing also presents potential challenges and limitations. Concerns regarding cybersecurity and scalability are notable (Karajovic et al., 2019; Rozario and Thomas, 2019). Although blockchain technology is generally viewed as secure against hacking and manipulation, the risk of a 51% attack, where a single group controls a majority of the network's computing power, and the loss or theft of private keys to digital wallets pose significant cybersecurity threats (Coyne and McMickle, 2017; Rozario and Thomas, 2019).

Furthermore, recording transactions on the blockchain does not necessarily confirm that the transaction has occurred in the real world, highlighting the necessity for regulatory support to prevent the misuse of blockchain and smart contracts (Alles and Gray, 2020; Dai and Vasarhelyi, 2017). Schmitz and Leoni (2019) also argue that blockchain has limited capabilities to detect fraudulent financial transactions from the beginning.

Scalability is another issue, particularly for public blockchains. Low transaction throughput and high consumption of storage and computational resources limit scalability and require further development for widespread adoption (Smith and Castonguay, 2020; Toufaily et al., 2021; Peters and Panayi, 2016). Additionally, the complexity of auditing blockchain-based assets and the lack of required knowledge and skills among auditors pose significant challenges (López-Pimentel et al., 2021).

7 Research gap

7.1 Integration with existing systems

Integrating blockchain technology with existing accounting and auditing systems is a significant challenge. The decentralization and immutability of blockchain can significantly improve the transparency and security of the audit process. However, seamless integration with existing systems is essential to maximize their benefits. Alarcon and Ng (2018) highlight limited research on best integration practices and addressing interoperability issues. This research gap is critical because interoperability issues can lead to inefficiencies and data inconsistencies that undermine the potential benefits of blockchain technology.

7.2 Continuous auditing and real-time reporting

Blockchain technology provides the ability to record and verify transactions in real time, providing an opportunity for continuous audit practices. Continuous audits allow for an ongoing assessment of financial transactions, providing more timely and accurate insights into the organization's financial health. However, Kokina et al. (2017) highlight that more research is still needed to develop methods and tools that enable auditors to conduct real-time audits effectively.

7.3 Valuation of cryptocurrencies

The valuation of cryptocurrencies remains a complex issue, and there is a limited understanding of their tax consequences, disclosure requirements, and regulatory framework. The volatile nature of cryptocurrencies such as Bitcoin and Ethereum poses a challenge to accurate valuations. Yermack (2015) highlights the need for research to develop new valuation methods and explore the impact of cryptocurrencies on financial reporting and auditing.

8 Conclusion

To sum up, blockchain technology is indispensable in the development of the times, especially when it comes to highly overlapping fields such as auditing. It can not only use its decentralization, non-tampering and traceability characteristics to solve the problem very well. It solves the problems that plague traditional audit evidence, such as low credibility, high audit costs and low efficiency. However, the technology has not yet been perfected. It is not only a technical issue, but talent cultivation must also be focused on. Despite this, large companies in the accounting industry have also initially used this technology, demonstrating its efficiency in auditing capabilities. Future research should focus on solving these issues: the safe use of blockchain, establishing a regulatory framework, detecting security vulnerabilities and adapting auditors to the technology. The solution to these problems is the key to ensuring that technology can be used in audits. From a national perspective, the law must formulate relevant guidelines and ethical frameworks to ensure that the technology is not abused by people with intentions to support the further development of blockchain. In short, blockchain technology not only brings new opportunities but also brings considerable challenges. To better use this technology, we will have a safer and more transparent audit environment in the future, reduce current technical risks, and fill regulatory gaps. It is an inevitable problem that blockchain will change the audit industry.

Author contributions

YZ: Writing – original draft, Writing – review and editing. ZM: Writing – original draft, Writing – review and editing. JM: Writing – original draft, Writing – review and editing.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Publisher's note

References

Alarcon, J. L., and Ng, C. (2018). Blockchain and the future of audit. *J. Emerg. Technol. Account.* 15 (1), 27–43. doi:10.2308/jeta-52220

Alles, M., and Gray, G. L. (2020). "The first mile problem": deriving an endogenous demand for auditing in blockchain-based business processes. *Int. J. Account. Inf. Syst.* 38, 100465. doi:10.1016/j.accinf.2020.100465

Arens, A. A., Elder, R. J., and Beasley, M. S. (2012). Auditing and assurance services: an integrated approach.

Atzei, N., Bartoletti, M., and Cimoli, T. (2017). "A survey of attacks on Ethereum smart contracts (SoK)," in *Proceedings of the 6th international conference on principles of security and trust*, 164–186.

Buterin, V. (2013). Ethereum white paper: a next-generation smart contract and decentralized application platform.

Christidis, K., and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access* 4, 2292–2303. doi:10.1109/access.2016.2566339

Coyne, J. G., and McMickle, P. L. (2017). Can blockchains serve an accounting purpose? *J. Emerg. Technol. Account.* 14 (2), 101–111. doi:10.2308/jeta-51910

Dai, J., and Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *J. Inf. Syst.* 31 (3), 5–21. doi:10.2308/isys-51804

Eyal, I., and Sirer, E. G. (2014). *Majority is not enough: Bitcoin mining is vulnerable in international conference on financial cryptography and data security*. Berlin, Heidelberg: Springer, 436–454.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., and Capkun, S. (2016). "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 3–16.

Gramoli, V., and Kuznetsov, P. (2018). "The unexpected vulnerability of decentralized consensus," in *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, 297–310.

Karajovic, M., Kim, H. M., and Laskowski, M. (2019). Thinking outside the block: projected phases of blockchain integration in the accounting industry. *Aust. Account. Review* 29 (2), 319–330. doi:10.1111/auar.12280

Kokina, J., Mancha, R., and Pachamanova, D. (2017). Blockchain: emergent industry adoption and implications for accounting. *J. Emerg. Technol. Account.* 14 (2), 91–100. doi:10.2308/jeta-51911

KPMG (2017). Digital ledger services at KPMG: seize the potential of blockchain today. Available online at: https://home.kpmg.com/xx/en/home/insights/2017/02/digital-ledger-services-at-kpmg-fs.html (Accessed March 3, 2017).

Li, Y., and Wang, Z. (2023). The current situation and suggestions for improvement of blockchain-related regulations in China. *Finance and Economics Research* 40 (2), 45–56.

López - Pimentel, J. C., Morales - Rosales, L. A., and Monroy, R. (2021). RootLogChain: registering log-events in a blockchain for audit issues from the creation of the root. *Sensors* 21 (22), 7669. doi:10.3390/s21227669

Low, A., Cao, C., and Wang, H. (2020). The impact of blockchain technology on the accounting profession: a review and research agenda. *Journal of Accounting Literature* 47, 1–16.

Messier, W. F., Glover, S. M., and Prawitt, D. F. (2017). Auditing and assurance services: a systematic approach.

Nakamoto, S. (2008). Bitcoin: a peer - to - peer electronic cash system.

Peters, G. W., and Panayi, E. (2016). *Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money*. Springer International Publishing, 239–278.

PWC (2017). Blockchain – an opportunity for energy producers and consumers? Available online at: www.pwc.com/gx/en/industries/assets/pwc-blockchain-opportunity-for-energy-producers-and-consumers.pdf (Accessed March 3, 2018).

Rozario, A. M., and Thomas, C. (2019). Reengineering the audit with blockchain and smart contracts. *Journal of Emerging Technologies in Accounting* 16 (1), 21–35. doi:10.2308/jeta-52432

Sabett, M. (2020). Identity and access management in blockchain: challenges and opportunities.

Schmitz, J., and Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: a research agenda. *Australian Accounting Review* 29 (2), 331–342. doi:10.1111/auar.12286

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* 17 (1), 119–131. doi:10.2308/jeta-52686

Sun, X. (2022). Research on the regulatory framework of blockchain technology in China. *Journal of Internet Law* 25 (3), 15–26.

Swan, M. (2015). Blockchain: blueprint for a new economy.

Tapscott, D., and Tapscott, A. (2016). Blockchain revolution: how the technology behind Bitcoin is changing money. *Business, and the World*.

Toufaily, E., Zalan, T., and Dhaou, S. B. (2021). A framework of blockchain technology adoption: an investigation of challenges and expected value. *Information and Management* 58 (3), 103444. doi:10.1016/j.im.2021.103444

Wang, X., Zhang, X., and Yang, G. (2021). A survey of identity management in blockchain-based internet of things. *Journal of Internet Technology* 22 (1), 201–214.

Yermack, D. (2015). "Is Bitcoin a real currency? An economic appraisal," in *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. Editor D. Lee (Elsevier), 31–43.

Yli - Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K. (2016). Where is current research on blockchain technology? a systematic review. *Peer - to - Peer Networking and Applications* 9 (3), 179–196.

Zhao, Y., Liu, X., and Zhang, Y. (2021). Research on the transformation and upgrading path of the accounting profession in the blockchain era. *Journal of Applied Accounting Research* 22 (2), 245–260.

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2019). An overview of blockchain technology: architecture, consensus, and future trends. *Future Generation Computer Systems* 97, 507–518.

Zyskind, G., and Nathan, O. (2015). "Enigma: decentralized computation platform with guaranteed privacy," in *Proceedings of the 2015 ACM SIGSAC conference on computer and communications security*, 399–410.