Deploying Blockchains to Simplify AI Algorithm Auditing

Ayesha Butt
Computer Science
SZABIST
Hyderabad, Pakistan
Ayesha.butt@hyd.szabist.edu.pk

Aisha Zahid Junejo
Computer and Information Sciences
Universiti Teknologi PETRONAS
Seri Iskandar, Malaysia
aishazj@gmail.com

Sumbul Ghulamani
Computer Science
SZABIST
Hyderabad, Pakistan
sumbul.ghulamani@hyd.szabist.edu.pk

Ghulam Mahdi
Kimberly Clark Corporation,
Roswell, GA, USA
Ghulam.mahdi@gmail.com

Asadullah Shah Kulliyah of Information and Communication Technology
IIUM, Malaysia
Asadullah@iium.edu.my

Dodo Khan
Computer and Information Sciences
Universiti Teknologi PETRONAS
Seri Iskandar, Malaysia
dodo_18001633@utp.edu.my

2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS) | 979-8-3503-2709-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICETAS59148.2023.10346420

***Abstract*—Artificial Intelligence has largely occupied various sectors in the world. A huge number of business companies have incorporated several machine learning algorithms for day-to-day decision making. With increasing applications of AI algorithms, the concerns regarding its outcomes have also increased due to bias. In AI algorithms, bias occurs due to multiple reasons including incomplete data, skewed data, human error and so on. These algorithms have the tendency to amplify partially and discrimination in the results instead of benefiting them. This makes it compulsory for the algorithms to be audited. Currently, AI algorithm auditing processes have several challenges including tendency of biases to be deeply ingrained into the system, making these difficult to mitigate; lack of transparency in decision making and many more. This study presents the emerging technology of blockchains to be a viable solution to the existing problem. It comprehensively discusses the suitability of blockchains for transparency in the process of algorithm auditing which is bound to easily capture the issue and the layer consisting it. Consequently, the process of algorithm auditing will be more convenient and more productive. Moreover, this review also discusses some potential challenges that need to be addressed and some future recommendations for this integration.**

***Keywords*— Algorithm Auditing, Algorithmic Bias, Blockchain Networks, Fairness in AI, Digital Transparency**

I. Introduction

Artificial Intelligence has largely occupied various sectors in the world. A huge number of business companies have incorporated several machine learning algorithms for day to day decision making. The goal of AI is to enable large enterprises take automated decisions that are faster, neutral, fairer and more efficient than the humans. These decisions are made after the machine is trained by the data fed into it. These algorithms often increase bias and prejudice in the results rather than improving them, depending on the quality of the data. [1]. Recently, increased scrutinizing has been witnessed in AI for ethical reasons including biased results, lack of transparency and data misuse. Consequently, distrust in AI is emerging. This makes it compulsory for the algorithms to be audited, as it will regain trust in AI. At present, the assessment of AI algorithms is not efficient. It is either very difficult to achieve, or very specific ideas are focused in those [2]. Currently, the biggest challenges with algorithm auditing are:

1) Tendency of biases to be deeply ingrained into the system, making these difficult to mitigate. As a result, these biases are potentially overlooked.
2) Lack of transparency in decision making of AI algorithms.
3) Increasing distrust in AI outcomes.

To solve these issues, this study proposes the emerging technology of the blockchain networks to be an accepted solution.

Blockchains is a decentralized ledger used for record keeping. It is the technology behind famous cryptocurrency like bitcoin, ethereum, NFTs, and more. Various features of blockchain such as data transparency, increased security, record immutability and user autonomy are the reason behind its wide adoption and increasing growth over the past few decades [3]. A number of domains such as healthcare, education, halal food industry, business, banking and finance have already incorporated blockchains in their day to day processes. This increased interest and acceptance for the technology motivated the idea of this study. In upcoming sections, the features of blockchain technology that make it a good solution for these problems are elaborated. Furthermore, the challenges of integration, such as scalability, privacy and security, along with regulatory compliance are also discussed. The major aim of this study is to provide a detailed review on existing issues with algorithm auditing and, applicability and benefits of blockchain for efficient and convenient auditing of AI algorithms. In the end, some future recommendations are also suggested by the authors for further study in this area.

II. Benefits of Using Blockchain for AI Algorithm Auditing

Blockchain networks are widely used in various applications due to their transparency and immutability [4]. The coming together of AI and blockchain has brought practical benefits. Blockchain keeps patient records safe in healthcare. AI studies patterns in this data for doctors to learn from. Together, they helped during COVID-19, like BurstIQ's health wallet [5]. Combining them revolutionizes finance with faster transactions and trust. Although these different, these help each other's weaknesses. These have many uses in 6G networks, smart cities, banking, and more. This combo distributes big data safely without a center authority, creating new applications. Blockchain [6] can store AI data due to its reliability. The article discusses merging blockchain with AI, focusing on practical uses and challenges before concluding. we'll explore the concept of using blockchains to streamline the process of auditing Artificial Intelligence (AI) algorithms [7]. To understand this idea completely, each component is explained individually as follows:

A. Blockchains:

Imagine a blockchain like a digital ledger or record-keeping system. It consists of a chain of interconnected blocks, each containing information. These blocks are linked together in a secure and transparent manner. The unique feature of a blockchain is that once information is recorded in a block, it cannot be easily altered, ensuring data integrity and security [8].

B. AI Algorithms:

Artificial Intelligence refers to computer systems that can perform tasks that typically require human intelligence. AI algorithms are sets of instructions that guide these systems to perform specific tasks or make decisions based on data analysis and pattern recognition [9]. It mimics the decision making process of a real human brain.

C. Algorithm Auditing:

Auditing [10] in this context means carefully examining and evaluating the performance, behavior, and outcomes of AI algorithms. This is important to ensure that AI systems are making accurate and fair decisions, especially in critical applications like healthcare, finance, or autonomous vehicles. Auditing helps identify biases, errors, or unintended consequences in AI algorithms.

Now, let's put these concepts together:

D. Deploying Blockchains for AI Algorithm Auditing:

By integrating blockchain technology into the process of auditing AI algorithms, several benefits can be achieved. Some of these are as follows:

1) **Transparency:**

Blockchains provide a transparent and tamper-resistant record of the steps taken by AI algorithms. Every action, decision, or data point processed by the AI is recorded in the blockchain. This transparency helps auditors and stakeholders understand how the AI arrived at a specific decision.

2) **Traceability:**

Since blockchains create an unchangeable history of events, auditors can trace back and review each step of the AI algorithm's decision-making process. The idea is similar to the one in [11] study. This is crucial for identifying errors or biases that may have influenced the algorithm's outcomes.

3) **Data Integrity:**

Information stored in a blockchain is highly secure and protected against unauthorized modifications [12]. This ensures that the data used by AI algorithms for decision-making remains accurate and trustworthy.

4) **Accountability**:

With blockchain-based auditing, the accountability of AI developers and organizations increases. They can't manipulate or hide information [13] about the AI's behavior, as all actions are recorded on the blockchain.

5) **Efficiency:**

The use of blockchain streamlines the auditing process. Auditors don't need to rely solely on the organization's reports; they can directly access the blockchain to verify the AI's actions. In summary, deploying blockchains to simplify AI algorithm auditing involves leveraging the secure, transparent, and tamper-resistant nature of blockchains to enhance the accuracy, fairness, and accountability of AI systems. This innovative approach has the potential to revolutionize how we ensure the reliability of AI algorithms across various industries.

III. Exploiting Blockchain Features for Artificial Intelligence

Various blockchain features can be exploited to make AI decision making more powerful. This section elaborates on how several processes on blockchain can provide assistance to AI algorithms.:

1) **Data Input and Processing:**

The AI algorithm processes data and makes decisions based on its programming and learning from the provided dataset. Every input data point, decision, and action taken by the AI is recorded as a transaction.

2) **Transaction Recording on Blockchain:**

Each transaction is added to a block in the blockchain. The block contains a cryptographic link (hash) to the previous block, creating a secure and unchangeable chain of blocks.

3) **Decentralized Verification:**

The blockchain is maintained by a decentralized network of nodes (computers). These nodes collectively verify and agree on the validity of transactions before adding them to the blockchain. Consensus mechanisms (like Proof of Work or Proof of Stake) ensure that fraudulent or inaccurate transactions are not added.

4) **Transparency and Traceability:**

Once a transaction is recorded, it cannot be easily altered or deleted due to the cryptographic links between blocks. Auditors can access the blockchain to view the entire history of data inputs, decisions, and actions taken by the AI algorithm. They can trace back and analyze each step of the algorithm's decision-making process.

5) **Data Integrity and Security:**

The information stored in the blockchain is highly secure and resistant to tampering. Even if an attempt is made to alter a transaction, it would require changing the entire subsequent chain, which is computationally infeasible.

6) **Real- time Monitoring and Analysis:**

Auditors can monitor the blockchain in real-time, ensuring that the AI algorithm is behaving as expected. Any deviations, errors, or biases can be promptly identified and addressed.

7) **Accountability and Audit Trail:**

The blockchain serves as an immutable audit trail that holds developers and organizations accountable for the behavior of their AI algorithms. Any unauthorized changes or attempts to manipulate the AI's decisions are readily detectable.

8) **Efficient and Trustworthy Auditing:**

Auditors can efficiently verify the AI algorithm's actions by directly accessing the blockchain, reducing reliance on potentially biased or incomplete reports from organizations.

9) **Continuous Improvement:**

Insights gained from auditing can be used to refine and improve the AI algorithm over time. The blockchain's historical data helps developers understand how the algorithm has evolved and identify areas for enhancement. In summary, the working mechanism of blockchain in auditing artificial algorithms involves recording every step and decision of the AI algorithm in a tamper-resistant blockchain. This transparency, traceability, and data integrity enhance the accuracy of audits, promote accountability, and provide a reliable tool for monitoring and improving AI systems.

IV. Existing Problems in AI Algorithm Auditing

Auditing AI algorithms at present face several challenges that may impact the effectiveness and credibility of the auditing process. Some of the problems include**:**

1) **Data Manipulation and Tampering:**

Without a secure and tamper-resistant ledger like a blockchain, there is a higher risk of data manipulation and tampering. Auditors may find it difficult to verify the authenticity and accuracy of the data used by AI algorithms, leading to potential biases or misleading results.

2) **Lack of Transparency:**

AI algorithms can be complex and opaque, making it challenging for auditors to understand how decisions are being made. Without a transparent record of each step taken by the algorithm, auditors may struggle to trace the decision-making process and identify potential issues.

3) **Limited Accountability:**

When auditing AI algorithms, it's crucial to hold developers and organizations accountable for the behavior and outcomes of the algorithms. Without a clear and immutable audit trail, it becomes harder to attribute specific actions or decisions to responsible parties.

4) **Incomplete Audit Trails:**

Traditional auditing methods might rely on documentation and reports provided by organizations. These reports can be incomplete, biased, or even intentionally misleading. Without an independent and comprehensive record, auditors might not have the complete information they need.

5) **Difficulty in Identifying Bias and Errors:**

Bias and errors in AI algorithms can have significant ethical and practical implications. Without a reliable method to track the algorithm's behavior, auditors may struggle to detect and rectify instances of bias or errors that could impact the algorithm's decisions.

6) **Manual and Resource-Intensive Auditing:**

Without automation and a secure data repository, auditing AI algorithms can become a manual and time- consuming process. Auditors may need to sift through vast amounts of data and documentation, increasing the likelihood of oversight or errors. Inefficient Dispute Resolution: In cases of disputes or disagreements about the behavior of AI algorithms, the absence of an immutable record can hinder the resolution process. Parties may lack a trustworthy source of information to refer to, making it difficult to reach a fair resolution.

7) **Difficulty in Tracking Algorithm Evolution:**

AI algorithms evolve over time as they are updated and retrained. Without a historical record of changes, it becomes challenging to understand how an algorithm has evolved and whether improvements have been made based on auditing insights.

8) **Lack of Trust and Confidence:**

Stakeholders, including customers, regulators, and the public, may have reduced trust and confidence in AI systems if the auditing process lacks transparency and reliability. This can hinder the adoption and acceptance of AI technologies. In conclusion, AI algorithm auditing without blockchain technology can lead to data integrity issues, limited transparency, challenges in accountability, and a less efficient auditing process overall. Integrating blockchain can help address these problems by providing a secure, transparent, and tamper-resistant platform for recording and verifying AI algorithm actions and decisions.

V. How Blockchain And AI Algorithms Auditing Link Together

Blockchain and AI algorithms auditing are linked through their combined capabilities to enhance transparency, accountability, and data integrity in the auditing process. Let's explore this connection in detail:

1) **Transparency and Traceability:**

Blockchain's transparent and immutable ledger records every action and decision made by AI algorithms. Auditors can trace back and verify each step of the algorithm's decision-making process, ensuring transparency [14].

2) **Data Integrity and Immutable Audit Trail:**

Blockchain ensures data integrity by preventing unauthorized alterations. Auditors can rely on the tamper-resistant audit trail in the blockchain to verify that data used by AI algorithms is accurate and has not been manipulated.

3) **Accountability and Attribution:**

Blockchain provides a trustworthy record of actions taken by AI algorithms. Developers and organizations can be held accountable for the behavior of their algorithms, as actions are immutably [15] linked to their origin.

4) **Auditing Automation and Efficiency:**

Blockchain automates the recording of AI algorithm actions, reducing manual efforts required for auditing. Auditors can efficiently access blockchain records for real-time monitoring [16] and analysis, enhancing the auditing process.

5) **Bias and Fairness Auditing:**

Blockchain helps in auditing AI algorithms for bias and fairness by providing an objective record of data inputs and decisions. Auditors can identify biased patterns in the blockchain data and assess the algorithm's fairness.

6) **Continuous Improvement and Evolution:**

Auditing insights from blockchain-recorded data can inform the continuous improvement of AI algorithms. Developers can analyze historical blockchain data to understand how algorithms have evolved over time.

The link between blockchain and AI algorithms auditing lies in their synergistic capabilities. Blockchain's transparency, traceability, data integrity, and automation enhance the auditing process for AI algorithms, making it more reliable, efficient, and accountable. This integration offers a robust solution for addressing challenges in auditing AI algorithms and ensuring their trustworthy and ethical behavior.

VI. BENEFITS OF AI ALGORITHM AUDITING WITH BLOCKCHAINS

Using blockchain for AI algorithm auditing offers several benefits that enhance transparency, accountability, and reliability in the auditing process.

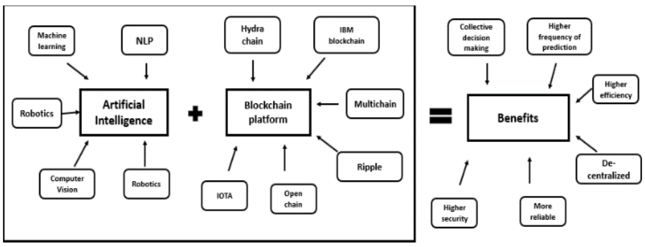

Fig. 1. Illustration of the application and benefits of Blockchain

Here are the advantages, along with relevant references for further exploration:

1) **Tamper-Resistant Audit Trail:**

Blockchain ensures that once data is recorded, it cannot be altered or deleted [17], providing an immutable audit trail of AI algorithm actions. Auditors can trust the accuracy and integrity of the recorded information.

2) **Transparency and Traceability:**

Every action, decision, and data input by the AI algorithm is transparently recorded on the blockchain. Using blockchain traceability feature [14] auditors can trace back and verify each step of the algorithm's decision-making process, enhancing transparency.

3) **Data Integrity and Authentication:**

Blockchain's cryptographic mechanisms ensure data integrity and authenticity. Auditors can be confident that the data used by AI algorithms has not been tampered with or manipulated [18].

4) **Automated Auditing Process:**

Blockchain automates the recording of AI algorithm actions, reducing the need for manual documentation. Auditors can efficiently access blockchain records for real-time monitoring and analysis, streamlining the auditing process.

5) **Bias and Fairness Auditing:**

Blockchain provides an objective record of data inputs and decisions, enabling auditors to assess bias and fairness. Auditors can identify patterns of bias in the blockchain data and evaluate the algorithm's ethical performance [19].

6) **Continuous Improvement Insights:**

Auditing insights from blockchain- recorded data inform the continuous improvement of AI algorithms. Developers can analyze historical blockchain data to understand the algorithm's evolution and refine its performance [20]. Incorporating blockchain into AI algorithm auditing offers a comprehensive solution that addresses challenges and enhances the credibility and effectiveness of the auditing process. These benefits collectively contribute to building trust in AI systems and promoting ethical and responsible AI development.

VII. CHALLENGES AND LIMITATION

While using blockchain for auditing artificial algorithms offers many benefits, it also comes with certain challenges and limitations. Let's explore these challenges along with relevant references for further understanding:

1) **Scalability:**

Blockchain networks can face scalability issues, especially when handling a large volume of AI algorithm transactions. High transaction throughput and processing can strain the network's capacity [21]. The study in [22] elaborates this issue on a deeper level. Interested readers may refer the study.

2) **Data Privacy and Confidentiality:**

Storing sensitive AI algorithm data on a public blockchain may raise privacy concerns. Ensuring data confidentiality while maintaining transparency is a challenge [23]. This problem is further discussed in [24].

3) **Smart Contract Vulnerabilities:**

Smart contracts used in auditing could have vulnerabilities that may be exploited by malicious actors, impacting the integrity of the audit process [12]. The study cited presents a deeper insight to this problem. Ensuring the security of smart contracts is essential [25].

4) **Consensus Mechanism Efficiency:**

Different consensus mechanisms (e.g., Proof of Work, Proof of Stake) have varying degrees of efficiency and energy consumption, which can impact the overall performance of the blockchain network. Selecting an appropriate consensus mechanism is crucial. For further study, please refer [26].

5) **Regulatory and Compliance Challenges:**

Integrating blockchain with AI algorithm auditing may raise regulatory challenges related to data governance, ownership, and compliance with industry standards. Navigating legal and regulatory frameworks is important.

6) **High Energy Consumption:**

Some blockchain networks, especially those using Proof of Work, can have high energy consumption, leading to environmental concerns. The environmental impact of blockchain operations is a limitation.

7) **User Adoption and Learning Curve:**

Implementing blockchain technology requires a learning curve for auditors and stakeholders unfamiliar with the technology. Ensuring user adoption and understanding is a challenge. Incorporating blockchain technology into AI algorithm auditing offers significant potential, but these challenges and limitations must be carefully considered and addressed to ensure a successful implementation.

VIII. DISCUSSION AND FUTURE TRENDS

The aim of this study is to review all the methods and techniques in auditing the AI algorithm with respect to blockchains. Several authors have focused on using blockchains to make AI algorithm audits simpler, and each has brought a different set of ideas and viewpoints to the conversation. According to some experts, blockchain technology can change the auditing process by supplying an immutable and transparent ledger for monitoring the actions and judgments of AI algorithms. The confidence among stakeholders and regulatory authorities is increased by this transparency. In their book "Blockchain Revolution," authors Don Tapscott and Alex Tapscott highlight how blockchain technology has the potential to build a tamper-proof audit trail for AI systems, assuring accountability and compliance. However, there are differing views as well. Critics point out challenges such as scalability, energy consumption, and the need for global consensus in blockchain networks. They argue that while blockchain offers transparency, it may not entirely eliminate the complexities of AI auditing, especially in cases where algorithms operate with sensitive or proprietary data. Consequences of these discussions include a growing awareness of the potential benefits and limitations of using blockchain technology for AI auditing. As the field continues to evolve, the insights from the authors play a crucial role in shaping the future of AI algorithm auditing and its integration with blockchain technology.

Future trends in auditing artificial intelligence (AI) algorithms with blockchain involves the integration of advanced technologies, regulatory developments, and increased emphasis on ethical and transparent AI practices. Let's delve into this trends:

1) **Multi-Stakeholder Verification and Transparency**

As AI algorithms continue to play a pivotal role in critical decision-making processes, the need for multi-stakeholder verification and transparency becomes more pronounced. Blockchain can facilitate collaboration among various stakeholders, including developers, auditors, regulators, and end-users, by providing a shared, immutable record of AI algorithm actions and decisions. This trend emphasizes the importance of involving diverse perspectives to ensure fair, ethical, and unbiased AI outcomes.

2) **Federated and Privacy-Preserving Auditing**

As concerns over data privacy and confidentiality grow, the trend of incorporating privacy-preserving techniques within blockchain-based AI algorithm auditing gains traction. Federated learning, where AI models are trained across decentralized devices while keeping data localized, can be combined with blockchain to enable auditing without exposing sensitive data.

3) **AI Algorithm Provenance and Explanation**:

This approach enhances security and encourages broader participation while maintaining data privacy Blockchain can be utilized to record the provenance of AI algorithms, capturing their evolution, training data, and decision-making processes. This trend aims to enhance algorithm accountability and provide detailed explanations for AI decisions, addressing concerns related to interpretability and bias. Blockchain's transparency helps in preserving a comprehensive history of algorithm behavior and associated explanations.

4) **Regulatory Compliance and Auditing Standards**

As the adoption of AI technologies increases, regulatory bodies are likely to establish standards and guidelines for AI algorithm auditing. Blockchain's ability to provide tamper-proof and auditable records can facilitate compliance with these regulations. This trend involves the alignment of blockchain-based auditing practices with evolving regulatory requirements.

IX. CONCLUSION

In this research paper, we conducted a thorough examination and assessment of the advancements of AI algorithms auditing the blockchains technology. The purpose of this study is to provide an overview of blockchain technology and its role in Auditing the AI algorithms. Additionally, this study also presents an extensive discussion, drawing comparisons among prevalent implementations of blockchain in terms of decentralized AI algorithms, infrastructure, and protocols. The paper also encapsulated the key features that AI brings to the realm of blockchain applications. Our comprehensive analysis highlights the nascent stage of integrating blockchain into AI applications. Several present research issues were identified, encompassing areas like privacy, security of smart contracts, reliable data sources, scalability, standardization, compatibility, resilience against quantum computing. This study is envisioned to encourage researchers and serve as a beginning point to further delve into this understudied application of Blockchain networks in AI, which could potentially change the entire landscape of AI at present.

ACKNOWLEDGMENT

The authors would like to acknowledge all their peers, professors and teachers for all the learning and guidance they have received for conducting this research work and other relevant work throughout their lives.

REFERENCES

[1] N. Kordzadeh and M. Ghasemaghaei, “Algorithmic bias: review, synthesis, and future research directions,” Eur. J. Inf. Syst., vol. 31, no. 3, pp. 388–409, 2022, doi: 10.1080/0960085X.2021.1927212.

[2] S. Brown, J. Davidovic, and A. Hasan, “The algorithm audit: Scoring the algorithms that score us,” Big Data Soc., vol. 8, no. 1, p. 205395172098386, Jan. 2021, doi: 10.1177/2053951720983865.

[3] A. Z. Junejo, M. Ahmed Hashmani, and A. Abdulrehman Alabdulatif, “Blockchain Privacy Preservation by Limiting Verifying Nodes’

During Transaction Broadcasting," in 2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Kuala Lumpur, Malaysia: IEEE, Jun. 2021, pp. 1–6. doi: 10.1109/ICECCE52056.2021.9514212.

[4] J. Teutsch and C. Reitwießner, "A scalable verification solution for blockchains." arXiv, Aug. 12, 2019. Accessed: Oct. 18, 2023. [Online]. Available: http://arxiv.org/abs/1908.04756

[5] G. Srivastava, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Data Sharing and Privacy for Patient IoT Devices Using Blockchain," in Smart City and Informatization, G. Wang, A. El Saddik, X. Lai, G. Martinez Perez, and K.-K. R. Choo, Eds., Singapore: Springer Singapore, 2019, pp. 334–348.

[6] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov, and Y. Koucheryavy, "On Performance of PBFT Blockchain Consensus Algorithm for IoT-Applications With Constrained Devices," IEEE Access, vol. 9, pp. 80559–80570, 2021, doi: 10.1109/ACCESS.2021.3085405.

[7] S. Jiang, K. Jakobsen, J. Bueie, J. Li, and P. H. Haro, "A Tertiary Review on Blockchain and Sustainability With Focus on Sustainable Development Goals," IEEE Access, vol. 10, pp. 114975–115006, 2022, doi: 10.1109/ACCESS.2022.3217683.

[8] B. C. Kaya, "The Role of Artificial Intelligence In Corporate Governance," SSRN Electron. J., 2022, doi: 10.2139/ssrn.4143846.

[9] A. Géron, Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems. O'Reilly Media, 2017. [Online]. Available: https://books.google.de/books?id=bRpYDgAAQBAJ

[10] A. Koshiyama et al., "Towards Algorithm Auditing: A Survey on Managing Legal, Ethical and Technological Risks of AI, ML and Associated Algorithms," SSRN Electron. J., 2021, doi: 10.2139/ssrn.3778998.

[11] K. Demestichas, N. Peppes, T. Alexakis, and E. Adamopoulou, "Blockchain in Agriculture Traceability Systems: A Review," Appl. Sci., vol. 10, no. 12, p. 4113, Jun. 2020, doi: 10.3390/app10124113.

[12] A. Z. Junejo, M. A. Hashmani, and M. M. Memon, "Empirical Evaluation of Privacy Efficiency in Blockchain Networks: Review and Open Challenges," Appl. Sci., vol. 11, no. 15, p. 7013, Jul. 2021, doi: 10.3390/app11157013.

[13] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, and L. Yalansky, "Ensuring data integrity using blockchain technology," in 2017 20th Conference of Open Innovations Association (FRUCT), St-Petersburg, Russia: IEEE, Apr. 2017, pp. 534–539. doi: 10.23919/FRUCT.2017.8071359.

[14] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," Comput. Ind. Eng., vol. 154, p. 107130, Apr. 2021, doi: 10.1016/j.cie.2021.107130.

[15] H. Han, R. K. Shiwakoti, R. Jarvis, C. Mordi, and D. Botchie, "Accounting and auditing with blockchain technology and artificial Intelligence: A literature review," Int. J. Account. Inf. Syst., vol. 48, p. 100598, Mar. 2023, doi: 10.1016/j.accinf.2022.100598.

[16] S.-C. Cha, W. Meng, W.-W. Li, and K.-H. Yeh, "A blockchain-enabled IoT auditing management system complying with ISO/IEC 15408-2," Comput. Ind. Eng., vol. 178, p. 109091, Apr. 2023, doi: 10.1016/j.cie.2023.109091.

[17] H. Altaş, G. Dalkiliç, and U. C. Çabuk, "Data immutability and event management via blockchain in the Internet of things," Turk. J. Electr. Eng. Comput. Sci., vol. 30, no. 2, pp. 451–468, Feb. 2022, doi: 10.3906/elk-2103-105.

[18] U. Bodkhe et al., "Blockchain for Industry 4.0: A Comprehensive Review," IEEE Access, vol. 8, pp. 79764–79800, 2020, doi: 10.1109/ACCESS.2020.2988579.

[19] R. Neisse, G. Steri, and I. Nai-Fovino, "A Blockchain-based Approach for Data Accountability and Provenance Tracking." arXiv, Jun. 14, 2017. Accessed: Oct. 18, 2023. [Online]. Available: http://arxiv.org/abs/1706.04507

[20] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," IEEE Access, vol. 7, pp. 10127–10149, 2019, doi: 10.1109/ACCESS.2018.2890507.

[21] A. I. Sanka and R. C. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," J. Netw. Comput. Appl., vol. 195, p. 103232, Dec. 2021, doi: 10.1016/j.jnca.2021.103232.

[22] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic Literature Review of Challenges in Blockchain Scalability," Appl. Sci., vol. 11, no. 20, 2021, doi: 10.3390/app11209372.

[23] O. Alfandi, S. Khanji, L. Ahmad, and A. Khattak, "A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues," Clust. Comput., vol. 24, no. 1, pp. 37–55, Mar. 2021, doi: 10.1007/s10586-020-03137-8.

[24] A. Z. Junejo, M. Ahmed, and A. Abdulrehman, "A Survey on Privacy Vulnerabilities in Permissionless Blockchains," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 9, 2020, doi: 10.14569/IJACSA.2020.0110915.

[25] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts".

[26] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija: IEEE, May 2018, pp. 1545–1550. doi: 10.23919/MIPRO.2018.8400278.