Blockchain for Artificial Intelligence: An Industry and Literature Survey

Ciprian Paduraru[1], Augustin Jianu[2] and Alin Stefanescu[1]
[1]*University of Bucharest, Romania*
[2]*Certsign, Bucharest, Romania*

Keywords: Blockchain, AI, Frameworks, Integration, Vehicular Networks Communication, 5G/6G Wireless Networks, Training Algorithms.

Abstract: The requirements of today's applications and their users set high demands and expectations. AI is a part of these and has played an important role recently. However, the credibility of AI methods is controversial in many cases, as is data security and user privacy. On the other hand, Blockchain is a trending technology that offers security and privacy as required by many enterprise applications. The presentation will provide an overview of how AI and Blockchain can be integrated for mutual benefit: (a) using Blockchains to make AI systems more trustworthy and private data secure, (b) using AI to improve Blockchain related operations and internal algorithms. The presentation includes examples from the literature, established research in the field, and practical examples from industry.

1 INTRODUCTION

Artificial intelligence (AI) and Blockchains are two of the most tending technologies used in various areas of software (Zhu et al., 2023). While AI is undeniably an area that can be used in almost every sector today, blockchains spread their use through many applications that require increased security, such as enterprise applications (Bandara et al., 2021), finance (Jain et al., 2021), Internet of Things (IoT) (Shammar et al., 2021), safety of automated vehicles (Alladi et al., 2020), (Narbayeva et al., 2020), home security (Ratkovic, 2022), medical systems (Abd-Alrazaq et al., 2021), metaverse (Huynh-The et al., 2023), supply chain management (Dutta et al., 2020), and many other areas as mentioned in the literature.

A *blockchain* (Shrimali and Patel, 2022) is, at its core, an immutable ledger that stores transactions. The main advantage of this technology is that the ledger is not stored in a centralized node, but is replicated across a group of peers and kept in sync at all times. Transactions between users are recorded and grouped into a linked list of blocks. The distributed and replicated ledger can store and exchange data in a cryptographically secure manner. The validity and security of data operations is ensured by so-called mining nodes. It has been proven both theoretically and empirically (Guo and Yu, 2022) that the data stored in the blockchain ledger has a high level of integrity and robustness and is almost impossible to manipulate. Due to features such as immutability, decentralization, cryptographic security, verifiability, etc., it has been used by various sectors. It started with applications for cryptocurrencies and financial applications in general, and then was adopted by sectors such as healthcare, Internet of Things (IoT), supply chain management, agriculture, etc. Smart contracts are pieces of software that can perform secure, programmed, and well-controlled actions on the blockchain. There are three main classes of blockchains: (a) Permissioned or Private blockchain (Vukolić, 2017): the platform can define and select participants and their roles. Generally used by industries and for private personal use. (b) Permissionless or Public (Bozic et al., 2016) blockchain: typically open source environments where any user can participate, e.g. Bitcoin, (c) Consortium blockchain (Li et al., 2017): a combination of the previous ones, usually used by a group of organizations that collaborate together on common projects or solutions. Each organization has its own access and rights attributes.

The goal of this paper is to analyze the research and applications presented in both academia and industry to find concrete examples of the merging of the two technologies, AI and Blockchains. There are three main research questions that we aim to answer in our work:

1. Can AI operations gain more trustworthiness and better train/query security by using blockchain as a foundation?
2. What is the friction/interface between merging AI and Blockchain operations in today's applica-

Paduraru, C., Jianu, A. and Stefanescu, A.
Blockchain for Artificial Intelligence: An Industry and Literature Survey.
DOI: 10.5220/0012147200003538
In *Proceedings of the 18th International Conference on Software Technologies (ICSOFT 2023)*, pages 712-719
ISBN: 978-989-758-665-1; ISSN: 2184-2833

tions.

3. Can the internal processes of blockchain technologies and frameworks be improved with the help of AI?

The remainder of the paper is organized as follows. Section 2 presents already implemented projects from industry that combine the two mentioned technologies. Section 2 presents ongoing research from the literature that answer our research questions but have not yet been implemented in practice. However, they provide an isolated and trustworthy evaluation. The final section provides discussion, conclusions, and some identified research gaps.

2 APPLICATIONS FROM INDUSTRY THAT COMBINE AI AND BLOCKCHAINS

Hanover [1] (Bohr and Memarzadeh, 2020), (Tagde et al., 2021), is a Microsoft AI technology that uses artificial intelligence to analyze existing health data and make recommendations. The method used is to process and store data collected from medical records to identify and suggest possible remedies for patients. The underlying method first analyzes the patient's personal health history information and then relates it to medical research publications. The output consists of general recommendations, therapies, treatments, etc. In this application, the blockchain acts as a platform for data storage and management. The patient data and the information obtained are then cryptographically secured and can be used by distributed systems for both consumption and storage in a secure manner.

In the same area, the pharmaceutical industry is using blockchain and AI to ensure that products are not counterfeited (Balan et al., 2022). Companies such as Sanofi, Pfizer, and Amgen are reportedly using a combination of these technologies to test, track, and ensure the security of their drugs' production chain from the research and development phase to market. Each drug is assigned a serial number, and any change or movement of that number is recorded in the general ledger. In this way, each unique serial number becomes fully traceable.

In agriculture, blockchain and AI are reported to be used for supply chain and decision-making system, as is the case with Heifer International [2]. The system behind this combines the predictive power of AI with data collected from geospatial, weather, environmental, and sensors connected as an Internet of Things (IoT) ecosystem. The AI systems are then able to provide future weather information, optimal cropping patterns by area, prices in different markets and regions, etc. The blockchain is able to collect and store the data in a decentralized manner, provide proof of origin for the produce, and ensure data security.

Financial services such as banking (Cucari et al., 2022) and cryptocurrency tracking applications in general (Yadav et al., 2022) were the first proponents of blockchain technology to ensure the security of their operations. In addition, the link between AI and blockchains is also being reported by investment and trading companies such as Webull: Investing and Trading[3], and Robinhood: Commision-free Stock Trading & Investing[4]. In this area, the security of data, identities, and transactions is provided by the blockchain. On the other hand, with the development of AI methods based on blockchain technology, there is greater confidence in the resulting automated processes, assessments, and recommendation engines. In this area, it is important to know that both data and AI models are stored on the Blockchain to ensure the security and traceability of the processes.

Another interesting use case of AI and blockchain working together is reported by IPwe[5]. The combination of these two technologies has helped them build an automated, transparent global patent registry (GPR). The purpose of this registry is to remove barriers to the collection, understanding, trading, and management of intellectual property (IP). Blockchain helps in two ways: (a) for records, data storage and smart contracts based automation services over the underlying IP assets, (b) to increase trust in the automated processes, assessments, and recommendations of AI systems.

3 RESEARCH AND FUTURE DIRECTIONS FROM SCIENCE

This section presents several suggestions and research from the literature that have been empirically tested but not yet applied in practice. We believe these are also important as they may suggest future use cases and attract industry partners and founders.

[1] https://www.microsoft.com/en-us/research/project/project-hanover

[2] https://www.heifer.org/

[3] https://www.webull.com/

[4] https://robinhood.com/us/en/

[5] https://ipwe.com/

3.1 An Architecture for the Convergence of AI and Blockchain

In the work of (Muheidat and Tawalbeh, 2021) authors define an architecture that combines AI and Blockchain operations along with stakeholder contributions and roles. A sketch of their proposals is shown in Fig. 1. The proposed architecture consists of three layers. In the *Contributors Layer*, stakeholders can collaborate and share datasets and AI models, and provide validation, analysis, and prediction tools. A concrete example from the medical domain might be that the stakeholders are a consortium of different hospitals. The different facilities can then add their data and records on patients and treatment correlations, which can be further used by predictive models to discover similarities and patterns for better decisions, research and recommendations in the future. The second layer, *Blockchain layer*, is a service-based layer that handles data storage, ledger management and transaction management, communication, connections between miners, role management, encryption of data, etc. These functions typically associated with the blockchain are encapsulated (hidden) in this layer to ensure separation of concerns from other stakeholders. The third layer, *User layer*, contains the users who are allowed to interact with the system. Following the example from the medical domain, the stakeholders in this case can be physicians, patients, and others who can access the datasets, models, and AI-based tools provided by the system.

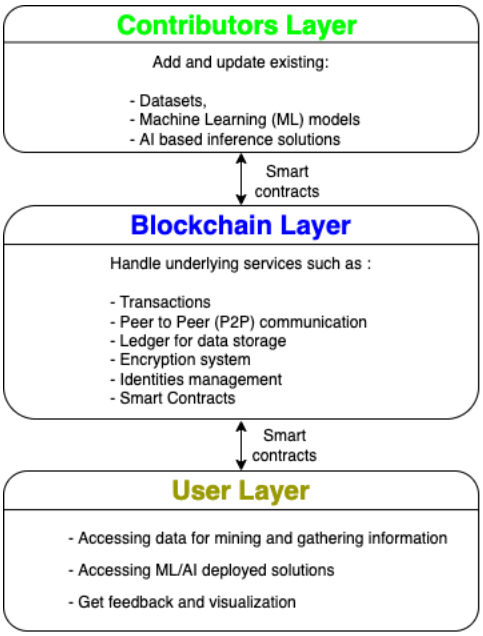

Figure 1: A foundation architectural proposal for the convergence of AI and blockchain solutions based on the work presented by (Muheidat and Tawalbeh, 2021).

3.2 Autonomous Vehicles Safety

Recent trends show a growing interest for Vehicular ad-hoc networks (VANET) and Vehicular Social Networks (VSN) (Lee and Atkison, 2021), (Azam et al., 2021). The main goal of vehicular communication systems is to enable peer-to-peer communication between vehicles, connect them to smart cities and sensors, and then use AI-based predictive algorithms to reduce traffic congestion and increase driver safety (Figure 2).

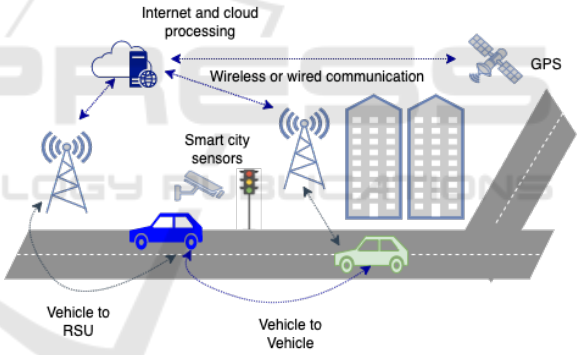

Figure 2: An illustration of how vehicles communicate within a smart city (V2X). They can communicate either directly, peer to peer (P2P), or with the urban infrastructure through the Road Side Units (RSU). All the data coming from the vehicles and the sensors installed in the city (cameras, traffic lights, etc.) can be stored in the cloud, processed and used by the authorized users.

However, this growing interest in vehicular communication systems has raised several potential attack methods aimed at modifying the content sent between vehicles or from the smart city to the vehicles in a way that disrupts predictive capabilities. In this sense, recent literature has made an interesting progress in this field, as shown by the works of (Bendiab et al., 2023), (Hammoud et al., 2020) and (Pokhrel and Choi, 2020). The solutions used by the authors generally combine AI prediction capabilities and algorithms with blockchains to secure intelligent automated vehicles (AVs). Secure messaging that combines these two technologies is also proposed in the work of (Malik et al., 2020).

Various types of attacks can occur in these scenarios, and a comprehensive list can be found in the work of (Azam et al., 2021). Common examples can be seen in Fig. 3. Data manipulation-based attacks, where the attacker gains authorized access to AVs to compromise data integrity and violate their privacy, are also very common in practice. Each AV is identified with a unique identifier that can help identify AV

and the flow of messages sent, but false identities can be created by attackers to influence the prediction results of the AI-based method (Bendiab et al., 2023), (Pokhrel and Choi, 2020).

From the existing research on these AV communication problems, we conclude that the intersection of blockchain and AI technologies can offer two main features:

- The ability to protect users' private data from cyberattacks.
- Decentralized access to data as it might be needed for the efficiency of AI systems.

An architecture in this sense is presented in (Hammoud et al., 2020), and outlined in Fig. 4. Vehicles can communicate directly or through a master node. Road data and sensors are generated and aggregated by the nearest RSUs (data generation layer). Finally, all communication at this layer is stored, processed, and validated by the nearest cluster where a blockchain ledger infrastructure is deployed (edge layer). This data is passed to the cloud layer, where predictive AI models are stored and continuously trained with new data. These models are sent back through the hierarchy to the data generation layer so that vehicles, traffic lights, and other entities can work together to reduce traffic congestion and ensure road safety.

As mentioned in the literature review, for the consortium of blockchain architecture deployed in the edge layer it is recommended to use the Byzantine Fault Tolerance protocol (Li et al., 2021) for consensus. The smart contracts that operate between the two lower layers are classified into three categories:

- Participant Authentication.
- Data Storing: collecting and storing data.
- AI models management between entities.

Training Automated Vehicles. In the same area, we identified the work in (Gandhi and Salvi, 2019) discussing a possible method for safely training automated vehicles. As noted in the paper, autonomous vehicles typically learn to drive using a variety of reinforcement learning methods. Vehicles could be connected to a shared public ledger to collect and share experiences (e.g., pairs of observations, rewards, and/or actions performed by a human expert) in a safe and reliable manner.

The conclusion of this study on vehicle communication is that the use of a blockchain layer would bring two main benefits to the AI systems built on top of it: (a) increasing the trust and reliability of the collected experience data, (b) better explaining the decisions of the AI algorithms, since the data can be stored and tracked in the blockchain.

3.3 5G/6G Wireless Networks and IoT

The architectural proposals presented in the previous section are continued in the work of (Li et al., 2020), (Dai et al., 2019), which further extends the concepts, architecture, and algorithms to combine AI and blockchain in the context of 5G and future 6G networks. The key foundation of their work is the observations that: (a) Blockchain is capable of providing a secure and decentralized resource sharing environment for different participating entities, (b) AI can solve specific problems in this domain involving uncertainty and time-varying characteristics, (c) finally, the integration of both can improve the performance of wireless networks.

An important architectural change from the previous one, shown in Fig. 4, is the caching mechanism, where the edge layer servers not only provide AI-based distributed intelligent wireless computation and routing, but also provide a caching mechanism to store computationally intensive and delay-sensitive applications (e.g., emergency situations, news, weather reports, etc.). The motivation for the caching mechanism is that the content generated by sensors, multimedia applications, traffic lights, etc., grows exponentially and challenges the transmission and processing capacity of the networks. In this sense, two roles are assigned: (a) a caching requester - e.g., a personal mobile device that needs to be notified from time to time in order for the owner to interact with a smart city environment, (b) a caching provider - a device capable of processing caching results or even receiving computing power. The edge layer servers have an AI algorithm (based on reinforcement learning) that is able to predict the communication patterns between the cache requestors and providers to optimize the overall process.

The blockchain is tasked with recording and validating all transactions generated in the wireless network, which in turn can enhance the security and privacy of the wireless ecosystem. As with the other examples shown previously, it also enables trustworthiness in AI data mining processes and decisions. For example, in the caching mechanisms presented above, each caching request or response generates a transaction that is then written to the blockchain. The blockchain receives these transactions and uses them to create blocks that are stored in the immutable ledger data structure. This would also allow providers to securely market different services in a smart city.

Indoor Positioning With 5/6G Wireless Networks. An interesting application of wireless networking is indoor positioning and pathfinding, such as a person in a shopping mall. Ideally, you would like to see

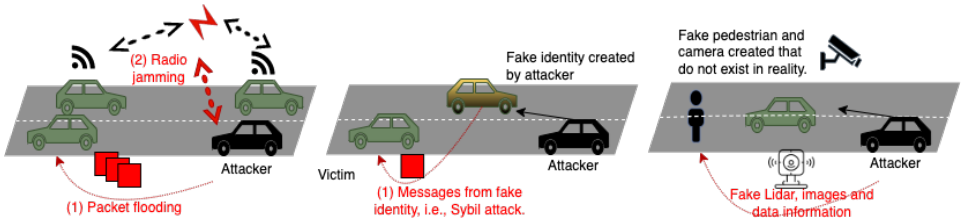

Figure 3: Common attacks in V2X scenarios, where the black vehicle is the attacker while the victims are colored green. The left figure shows a Denial of Service attack (DoS), where the attacker blocks wireless communications through message flooding and radio jamming. In the middle figure, a fake identity is created to send fake messages (Sybil attack). The figure on the right contains an example of creating fake entities such as vehicles, cameras, or pedestrians to send false or disrupted information to the victim.

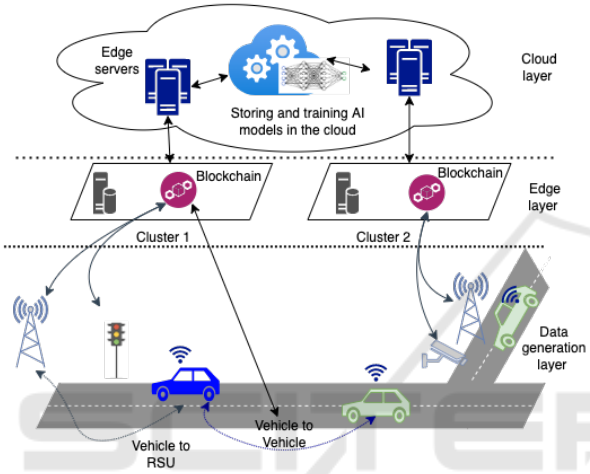

Figure 4: A vehicle communication network as a typical IoT system, with three layers: the data generation, edge and cloud layers.

where you are on the map of the mall and how to get to specific locations inside (Wang et al., 2020). There are many known algorithms for indoor positioning and pathfinding using AI methods. However, in general, AI methods operate in a centralized manner, while in this case the required operations are decentralized. The main research question in this context is how a system can solve the queries from different users in a *safe* and *decentralized* world.

The chosen solution is to integrate AI and blockchains. There are two roles in this system: (a) The *requester*: a set of people who request location information, e.g., by sending locations with their phones and trying to find specific areas, (b) The *worker*: can provide localization and pathfinding services to requesters. An important note is that requesters should be able to provide feedback on the services they receive.

The key principles in the implementations are as follows:

- Define requests for a set of workers that can perform localization and pathfinding services.
- For each request, have an algorithm that selects a set of trusted workers to perform the operations.
- Use the blockchain to prevent malicious attackers (e.g., workers who try to create false identities or provide false information).

As shown in the architecture of the system in Fig. 5, the blockchain platform works as an intermediate layer between requesters and workers. It first solves the problem of decentralized data storage. Then, both entities can agree through transactions on the blockchain, which are added to blocks and stored in the ledger for traceability and auditability. The trusted authority (TA) designed for the blockchain platform is responsible for authorizing and validating the registration identities of participants without compromising privacy. This component would then allow the Blockchain to store data and transactions in a secure manner. The *Fog server* in this architecture, is playing the role of the computational node for blockchain operations such as consensus algorithms (i.e., it manages the group of miners), process feedbacks, and selects trusted workers based on their current reputation value (AI can help in this direction through regression or recommendation systems).

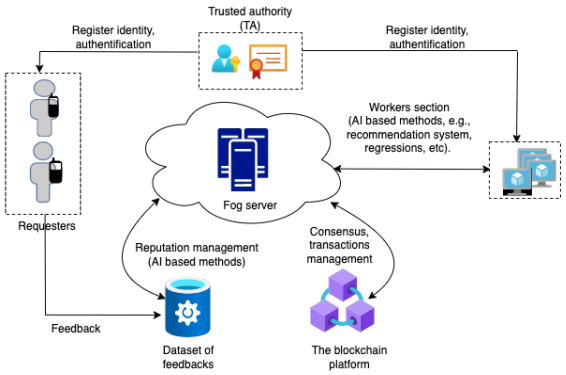

Figure 5: An architectural system of blockchain and AI working together to provide indoor localization and navigation services.

3.4 Using AI to Optimize Internal Blockchain Operations

As mentioned in Section 4, we believe that there are important research opportunities to leverage AI in the internal algorithms and mechanisms of the Blockchain. At the moment, we have noted two works in this area. In (Wang et al., 2021), the authors use reinforcement learning (RL) methods to optimize the mining strategy for a particular Bitcoin-like blockchain. The mining problem is modeled as a Markov decision process (MDP) and the RL agent trains on it. However, blockchain networks and parameters can change rapidly over time, which in general breaks the assumption that an MDP can be defined. The agent would then use policies learned based on incorrect/old data. The work in (Chen et al., 2018) proposes a neural network to select a set of nodes to participate in the consensus mechanism for each query. However, the proposal has not yet been formally proven or demonstrated by robust empirical experiments.

4 DISCUSSION AND CONCLUSIONS

AI algorithms and methods must use data or information to learn, interpret, and then draw conclusions. When this data comes from secure and trusted channels, machine learning algorithms can perform better and present their decisions with more credibility. This result is achieved by using blockchains as the underlying technology for data storage and management, which creates a secure, immutable, and decentralized system needed to improve AI methods that typically need to collect, store, and use sensitive data (IBM, 2023). Without blockchain support, it will be difficult to trust the data and decisions that come from AI-powered methods. Generally speaking, from a high-level architecture perspective, by building AI methods on top of blockchain technologies architecturally, the design and specification are moving from the tradition ones, as shown in Figure 6, to the specification given in Figure 7.

Smart contracts can enable both automated data retrieval and analysis using machine learning algorithms. The security of the underlying data and miners makes the results of their operations highly trustworthy.

As shown in the wireless network and vehicular communication studies in Section 2, the integration of the two technologies can enable intelligent decentralized autonomous agents (DAOs) to validate data

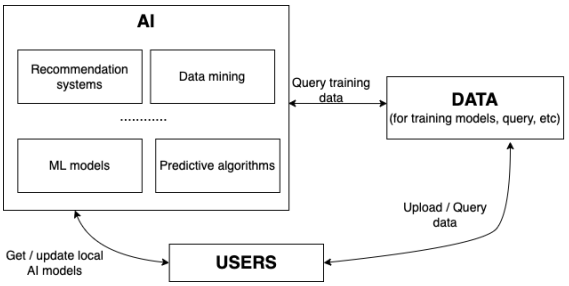

Figure 6: The traditional, centralized way of using AI methods for training, queries, and user interactions.

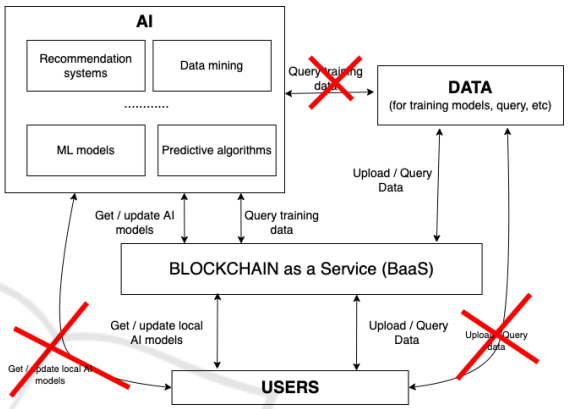

Figure 7: Combining AI and Blockchain technologies at a high level, in a departure from the traditional methods, as shown in Figure 6. The potential benefits would be decentralized AI services, more data security, trustworthiness, easier explanation and traceability of the results of AI methods.

and asset transfers, as well as AI-based predictive capabilities in IoT environments.

In this sense, we believe it may be a matter of time before the current research is applied in practice to obtain a better and more secure communication environment between people, smart cities, and vendors in general. In the gaps and research opportunities identified, we found that there is a lack of AI methods being used to improve operations within the Blockchain. We believe AI can also be used for optimized consensus mechanisms, predictive methods for selecting miners, and other internal entities involved in lower-level blockchain operations.

ACKNOWLEDGEMENTS

This research was supported by the European Regional Development Fund, Competitiveness Operational Program 2014-2020 through project IDBC (code SMIS 2014+: 121512).

REFERENCES

Abd-Alrazaq, A. A., Alajlani, M., Alhuwail, D., Erbad, A., Giannicchi, A., Shah, Z., Hamdi, M., and Househ, M. (2021). Blockchain technologies to mitigate covid-19 challenges: A scoping review. *Computer methods and programs in biomedicine update*, 1:100001.

Alladi, T., Chamola, V., Sahu, N., and Guizani, M. (2020). Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications*, 23:100249.

Azam, F., Yadav, S. K., Priyadarshi, N., Padmanaban, S., and Bansal, R. C. (2021). A comprehensive review of authentication schemes in vehicular ad-hoc network. *IEEE Access*, 9:31309–31321.

Balan, A., Alboaie, S., and Raţă, A. (2022). Pharmaledger a blockchain-enabled healthcare platform. In *2022 E-Health and Bioengineering Conference (EHB)*, pages 1–6.

Bandara, E., Liang, X., Foytik, P., Shetty, S., Ranasinghe, N., and De Zoysa, K. (2021). Rahasak—scalable blockchain architecture for enterprise applications. *Journal of Systems Architecture*, 116:102061.

Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N., and Shiaeles, S. (2023). Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. *IEEE Transactions on Intelligent Transportation Systems*, 24(4):3614–3637.

Bohr, A. and Memarzadeh, K. (2020). *The rise of artificial intelligence in healthcare applications*, pages 25–60. MIT online.

Bozic, N., Pujolle, G., and Secci, S. (2016). A tutorial on blockchain and applications to secure network control-planes. *2016 3rd Smart Cloud Networks & Systems (SCNS)*, pages 1–8.

Chen, J., Duan, K., Zhang, R., Zeng, L., and Wang, W. (2018). An AI based super nodes selection algorithm in blockchain networks. *CoRR*, abs/1808.00216.

Cucari, N., Lagasio, V., Lia, G., and Torriero, C. (2022). The impact of blockchain in banking processes: The interbank spunta case study. *Technology Analysis & Strategic Management*, 34(2):138–150.

Dai, Y., Xu, D., Maharjan, S., Chen, Z., He, Q., and Zhang, Y. (2019). Blockchain and deep reinforcement learning empowered intelligent 5g beyond. *IEEE Network*, 33(3):10–17.

Dutta, P., Choi, T.-M., Somani, S., and Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation research part e: Logistics and transportation review*, 142:102067.

Gandhi, G. M. and Salvi (2019). Artificial intelligence integrated blockchain for training autonomous cars. In *2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, volume 1, pages 157–161.

Guo, H. and Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: research and applications*, 3(2):100067.

Hammoud, A., Sami, H., Mourad, A., Otrok, H., Mizouni, R., and Bentahar, J. (2020). Ai, blockchain, and vehicular edge computing for smart and secure iov: Challenges and directions. *IEEE Internet of Things Magazine*, 3(2):68–73.

Huynh-The, T., Gadekallu, T. R., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q.-V., da Costa, D. B., and Liyanage, M. (2023). Blockchain for the metaverse: A review. *Future Generation Computer Systems*.

IBM (2023). Blockchain and artificial intelligence. *Internal report*.

Jain, D., Dash, M. K., Kumar, A., and Luthra, S. (2021). How is blockchain used in marketing: a review and research agenda. *International Journal of Information Management Data Insights*, 1(2):100044.

Lee, M. and Atkison, T. (2021). Vanet applications: Past, present, and future. *Vehicular Communications*, 28:100310.

Li, W., Su, Z., Li, R., Zhang, K., and Wang, Y. (2020). Blockchain-based data security for artificial intelligence applications in 6g networks. *IEEE Network*, 34(6):31–37.

Li, Y., Qiao, L., and Lv, Z. (2021). An optimized byzantine fault tolerance algorithm for consortium blockchain. *Peer-to-Peer Networking and Applications*, 14:2826–2839.

Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., and Zhang, Y. (2017). Consortium blockchain for secure energy trading in industrial internet of things. *IEEE transactions on industrial informatics*, 14(8):3690–3700.

Malik, N., Nanda, P., He, X., and Liu, R. (2020). Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology. *Wireless Networks*, 26.

Muheidat, F. and Tawalbeh, L. (2021). *Artificial Intelligence and Blockchain for Cybersecurity Applications*, pages 3–29. Springer International Publishing, Cham.

Narbayeva, S., Bakibayev, T., Abeshev, K., Makarova, I., Shubenkova, K., and Pashkevich, A. (2020). Blockchain technology on the way of autonomous vehicles development. *Transportation Research Procedia*, 44:168–175.

Pokhrel, S. R. and Choi, J. (2020). Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. *IEEE Transactions on Communications*, 68(8):4734–4746.

Ratkovic, N. (2022). Improving home security using blockchain. *International Journal of Computations, Information and Manufacturing (IJCIM)*, 2(1).

Shammar, E. A., Zahary, A. T., and Al-Shargabi, A. A. (2021). A survey of iot and blockchain integration: Security perspective. *IEEE Access*, 9:156114–156150.

Shrimali, B. and Patel, H. B. (2022). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. *Journal of King Saud University - Computer and Information Sciences*, 34(9):6793–6807.

Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., Kaushik, D., and Rahman, M. (2021).

Blockchain and artificial intelligence technology in e-health. *Environmental Science and Pollution Research*, 28.

Vukolić, M. (2017). Rethinking permissioned blockchains. In *Proceedings of the ACM workshop on blockchain, cryptocurrencies and contracts*, pages 3–7.

Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., and Zhou, W. (2020). Security and privacy in 6g networks: New areas and new challenges. *Digital Communications and Networks*, 6(3):281–291.

Wang, T., Liew, S. C., and Zhang, S. (2021). When blockchain meets ai: Optimal mining strategy achieved by machine learning. *Int. J. Intell. Syst.*, 36(5):2183–2207.

Yadav, S. P., Agrawal, K. K., Bhati, B. S., Al-Turjman, F., and Mostarda, L. (2022). Blockchain-based cryptocurrency regulation: An overview. *Computational Economics*, 59(4):1659–1675.

Zhu, J., Cao, J., Saxena, D., Jiang, S., and Ferradi, H. (2023). Blockchain-empowered federated learning: Challenges, solutions, and future directions. *ACM Computing Surveys*, 55(11):1–31.