frontiers | Frontiers in Blockchain

ORIGINAL RESEARCH
published: 04 July 2022
doi: 10.3389/fbloc.2022.927006

Artificial Intelligence for Demystifying Blockchain Technology Challenges: A Survey of Recent Advances

Olayemi Mikail Olaniyi[1]*, *Abraham Ayegba Alfa*[2] and *Buhari Ugbede Umar*[1]

[1]Department of Computer Engineering, Federal University of Technology, Minna, Nigeria, [2]Department of Computer Science, Confluence University of Science and Technology, Osara, Nigeria

Blockchain technology has gained lots of traction in the past five years due to the innovations introduced in digital currency, the Bitcoin. This technology is powered by distributed ledger technology, which is a distributed database system. It is often renowned for decentralization, anti-attack, and unfalsified attributes making it a top choice in several non-monetary applications. In fact, the problem of privacy and security of the Internet of Things has been undertaken aggressively with Blockchain. Several problems have been identified with blockchain technology such as large delays and lack of support for real-time transaction processing, authorization, node verification, and consensus mechanisms. This article intends to provide a comprehensive survey on the recent advances and solutions to the problems of blockchain technology by leveraging the artificial intelligence approaches. The outcomes of this study will provide valuable information and guidance on the design of Blockchain-based systems to support time-sensitive and real-time specific applications and processes.

Keywords: blockchain technology, artificial intelligence, real-time, Internet of Things, distributed ledger technology, weaknesses, solutions

OPEN ACCESS

Edited by:
Kavita Saini,
Galgotias University, India

Reviewed by:
Chellammal Surianarayanan,
Bharathidasan University, India
KM. Bala,
Galgotias University, India

****Correspondence:***
Olayemi Mikail Olaniyi
mikail.olaniyi@futminna.edu.ng

Specialty section:
This article was submitted to Blockchain Technologies, a section of the journal Frontiers in Blockchain

Received: *23 April 2022*
Accepted: *30 May 2022*
Published: *04 July 2022*

Citation:
Olaniyi OM, Alfa AA and Umar BU (2022) Artificial Intelligence for Demystifying Blockchain Technology Challenges: A Survey of Recent Advances. Front. Blockchain 5:927006. doi: 10.3389/fbloc.2022.927006

INTRODUCTION

The prospects of blockchain technologies became pronounced shortly after the launch of Bitcoin, the online cryptocurrency, in 2008. The operation of the blockchain is based on a decentralized and distributed ledger system maintained by every node on the network. There is no central authority for managing transactions due to the concept of immutability placed on transactions, which implies no tampering or overwriting of the ledger once committed. The storage or database is safe and secured through strong hashing cryptography. Every transaction is linked to another; thereby increasing transparency and security of information. There are complete and comprehensive transaction logging systems on Blockchain. The process of writing and reading to the blockchain are consensually attained rather than a set of nodes (Hassan et al., 2019; Alfa et al., 2021a).

The intention of Szabo's smart contracts is to design computer-based protocols that autonomously support, enhance, verify and carry out digital contracts and negotiations entered between individuals or parties without the need for central establishments such as Hyperledger and Ethereum. In effect, blockchain technology uses smart contracts in the digital economy, intelligent manufacturing and industries, medicine, financial management, Internet of Things (IoT), and the list is inexhaustive. Aside immaturity of blockchain technology, security and privacy are the topmost technical hurdles to be scaled (Wang et al., 2019). The blockchain networks are usually complex, the quest to have lightweight clients capable of running mobile interfaces is desirous. This is capable of increasing the application frontiers of this technology (Mukkamala et al., 2018).

Artificial intelligence (AI) is a field of computer science responsible for the design and execution of tasks initially undertaken by humans. However, these tasks are often repetitive and well defined (Yang and Yu, 2021). AI was developed to accumulate and identify information of interest within a stockpile of data generated from events. The emergence of AI brought about smart environments. Though, the merger of blockchain technology and AI has been a long subject of investigation by the research community (Azzaoui et al., 2020). Several variants (such as the deep convolutional neural network) of AI have been successful in diverse areas of applications including natural language processing, and computer vision. (Zhang et al., 2019). This survey underpins the contributions of both technologies (that is, blockchain technology and AI) to resolving the challenges of the former. The contributions of this study include the following: 1) To identify current challenges of blockchain technology. 2) To discuss the recent methods of AI for demystifying these challenges in blockchain technology. 3) To highlight the cases, scenarios, and prospects of AI in blockchain technology.

BLOCKCHAIN TECHNOLOGY

The Basis of Blockchain Technology

The origin of blockchain can be traced to a pseudonym, Satoshi Nakamoto, during a forum on the bitcoin in the year 2008 entitled Bitcoin: A Peer-to-Peer Electronic Cash System. This technology motivated several revolutions in industry and technology. The concept of blockchain technology enables distributed ledger systems, intelligent consensus contracts, asymmetric encryption, and numerous core technologies. Blockchain is the backbone technology for digital cryptocurrencies such as Hyperledger, Bitcoin, and Ethereum. Blockchain offers point-to-point, traceability, anonymity, tamper-proof, trust, and security of transactions. Aside from the financial sector, other application areas of blockchain include the Internet of Things (IoT), edge computing, supply chain management, and Artificial Intelligence (Wang et al., 2020).

The blockchain is a database on an append-only structure and operated by the peer-to-peer (P2P) nodes on its networks. It is composed of three key layers including the peer-to-peer network backbone, databases, and associated applications. In this case, the communication process is managed by a P2P network, every node has an equal right to provide and consume information. More so, is the routing process of the network (that is, discovering and establishing connections to adjoining nodes) (Feng et al., 2019). While the global ledger controls the message transmission across addresses assigned to users in form of cryptographic-based public-private keys (Feng et al., 2019).

Strengths of Blockchain Technology

The trustless nature of blockchain technology emboldens the consensus mechanism in which nodes on the entire network must reach an agreement on authorizing or verifying transactions. Though, the information contained in blocks becomes public due to the disclosure policy of the chain, which raises privacy challenges for the users. However, blockchain is a kind of distributed database that enforces privacy protection through a decentralized structure and data storage mechanism. These offer information tamper-proof, stability of the network, and anonymity in attempts to overcome the issue of privacy disclosure often faced in centralized services, especially in blockchain-propelled voting systems, and intelligent parking lot systems (Wang et al., 2020; Feng et al., 2019).

Blockchain technology uses distributed verification of transactions process in that large amounts of miners collaborate in verifying the legitimacy of the transaction prior to appending it to the blockchain. In case of the inconsistent state of the blockchain, all the nodes update their local copy of the blockchain with the state on the basis of the consensus of miners, that is, the exact state of the blockchain is attained through the election. However, this approach is weak to the attacks such as sybil (Conti et al., 2018). Chatterjee and Chatterjee (2017) enlisted the key benefits of blockchain including irreversible (double spending resistant), immutable (tamper-proof), distributed system (participants retain a copy of ledger), resilient (less prone to common attacks), and trustless (peer-to-peer system rather than central authority).

ARTIFICIAL INTELLIGENCE

The science targeted at evolving machine systems capable of exhibiting intelligence similar to the mind of humans is known as Artificial Intelligence (AI). It can be used to crack complex tasks autonomously without interference by humans. AI can be broadly classified into natural language processing, and machine learning approaches. Natural language processing (NLP) assists humans to interrelate with computers through specialized natural language. NLP understands, deciphers, and comprehends human language in special ways. Machine learning attempts to explain the interrelationship between input and output for the purpose of deducing primary needed for future forecasts on the basis of acquired patterns (supervised learning) or identifying clusters of data from input values (van Klompenburg et al., 2020). Though, deep learning has advanced the applications of AIs by means of optimization processes. In fact, deep learning replicates the functions of the human brain by acquiring knowledge autonomously from unlabeled and unstructured data (Azzaoui et al., 2020; van Klompenburg et al., 2020).

In particular, deep learning is applied to high-dimensional data to explain the interrelationships as in the case of, object detection, image classification, and semantic segmentation. Convolutional neural network (CNN), Recurrent Neural Network (RNN), Long-Short Term Memory (LSTM), and Radial Basis Function Network (RBFN) are some forms of AI's deep learning subcategory (Yang and Yu, 2021). A water management and control station using RBFN was developed for the purpose of predicting water level, weather, and irrigation parameters (Adenugba et al., 2019). The rate of yield of the crop was undertaken with AI's machine learning subcategories such as deep neural networks, LSTM and CNN. The global markets return forecasting was accurately determined through machine

learning methods (Al- Sulaiman and Al- Matouq, 2021). AI is used to improve medical decision-making processes, diagnosis, and treatment of chronic diseases (Battineni et al., 2020). AI-based trust management for security and resource allocation on critical health networks/applications (Abbasi et al., 2021).

PROBLEMS OF BLOCKCHAIN TECHNOLOGY

A peer-to-peer technology-based cryptographically secure electronic payment platform was investigated by Conti et al., (2018), which allows virtual currency (known as Bitcoin) to be traded. Bitcoins arouse interest from researchers and industry players due to their huge market capitalization and increased transaction pull on daily basis. These attracted all manners of attacks including double spending, net-split, the malleability of the transaction, networking attacks, and mining pools. Anonymous digital currency and decentralized networking (such as blockchain and consensus protocols) are mostly used in Bitcoin which removes backtracking property, central controls, and increased openness. Two algorithms have been proposed for the Bitcoin system for privacy protection of users' transactions including proof-of-work and consensus; but, are unable to resist manipulations and stop certain kinds of attacks. However, there is a need to focus, in future works, on user privacy and anonymity issues in the e-commerce industry.

One of the topmost cryptocurrencies is the Bitcoin in which all transactions are kept in a distributed append-only public ledger known as the blockchain. Bitcoin is majorly protected through incentive-well-suited proof-of-work using distributed consensus protocol run by miners (network nodes). In reward for the incentive, the miners are required to fairly preserve the blockchain. Since its unveiling in 2009, Bitcoin has amassed a stupendous growth rate and is valued at several billions of dollars. But, the unprecedented progress in the economy of Bitcoin has given rise to threats from adversaries in attempts to exploit weaknesses for profit-making purposes; therefore, researchers are expected to reveal fresh vulnerabilities in this system. In addition, Bitcoin's normal functionality can be distorted due to the vulnerabilities of Proof-of-Work and blockchain (Conti et al., 2018).

A number of advantages can be derived from blockchain technology, especially in providing distributed things security services [Salman et al. (2019)] including confidentiality, privacy, provenance, authentication, and integrity. The authentication and confidentiality solutions are attainable through the public-private key cryptography such as encryption and the signature approaches. However, there is no practical experimentation of different blockchain approaches in large-scale and real-world situations for performance assessments. Ferrag et al. (2018) highlighted various blockchain protocols in IoT networks. In particular, these protocols have been applied in Vehicles, Energy, Cloud, and Edge computing. Blockchain-IoT network protocols are vulnerable to threats such as identity, manipulation, cryptanalytic, reputation, and service. New solutions are expected to be evolved for special blockchain infrastructure, vehicular cloud advertisement broadcast, and Skyline query processing, trust management, and resiliency against threats.

Blockchain technology is an important part of the cryptocurrency Bitcoin because of its decentralized and falsified properties (Yang et al., 2018). The Blockchain's distributed and anti-attack nature makes it suited for more advanced applications, especially in IoT systems. These technical properties of blockchain enable distributed privacy and security solutions for IoT systems. Blockchain technology provides less-expensive links and direct exchanges among several IoT devices. Though, IoT and blockchain are distinct technologies whose integration may give rise to new challenges. Most significantly, there is the prospect of advancing both technologies in improving the well-being of people globally through the automation of everyday activities.

Data compromises and corruption are largely responsible for the vulnerability of smart places (Brandão et al., 2018)). Moreover, the false integration of new devices and devices running on inconsistent firmware versions will continue to increase risks in addition to the huge pile of data, devices, infrastructures, and end-users available on the Web. Notwithstanding the applications of blockchain in IoT, serious issues abound including security focus (confidence, privacy, scalability, and anonymization); scalability (applications require huge power for computing, verification, and confirmation of transactions); unrestricted access to information (transactions are consummated in public for transparency open identification and backtrack); and data management (centralized service provision to be replaced with a decentralized scheme to eliminate third party controls).

Feng et al. (2019) understudied the possible setbacks for the widespread deployment of Blockchain, in which privacy risks is topmost. The general acceptance and awareness of blockchain technology are associated with the decentralized nature and security; as well as a unique mode of storing, sharing, and updating data which is the direction of most upcoming Internet interactive systems such as IoT or supply chain systems. It was discovered that most of the deployed data privacy preservation techniques were based on cryptography for anonymity and transaction privacy only. However, there is a need to evolve conditional methodology for a trusted authority to backtrack users and transactions while hiding the personal data of users in the blockchain network. More so, new privacy protection methods must reduce the overheads due to communication, waiting for delays, and complex computations, especially in non-scalable anonymity sets. The author drew the future efforts in three aspects to include: 1) Obfuscation on the transaction associations to prevent backtrack analysis. 2) Concealing the identities of the sender and the receiver identities by mean complex cryptographic primitives. 3) Blinding the transaction content but, their verifiability and computability are reserved.

Blockchain technology is limited by the one-mode of transaction phenomenon; that is, only one type of asset can be operated at a time, while there is a lack of specified amounts of

nodes required to attain consensus for transaction approval. This causes enormous time wastage and process slowness on the blockchain (Chatterjee and Chatterjee, 2017). Though there are several upcoming applications motivated by Blockchain, its performance and architecture can be improved subsequently. Notwithstanding, interoperability and scalability problems of blockchains still persist (Ensor et al., 2019) in its subcategories such as public, private, and consortium.

POTENTIAL SOLUTIONS OF ARTIFICIAL INTELLIGENCE

AI can be significantly applied to overcome the problem of threats and vulnerabilities through effective auditing of blockchain assets and resources (Alfa et al., 2021b). The smart contract refers to the collection of promises generated digitally alongside a collection of rules to guide parties in fulfilling their promises (Wang et al., 2019). AI can be used to adequately control the operations of the consensus mechanisms and protocols in blockchain (Conti et al., 2018). The hash functions are used to generate block hash in order to resist attack as shown in the following equation:

$$y = 2^r, \tag{1}$$

where, r = 256, 384, 512 bits long in present-day blockchains, which must exceed the hashing value of y for every r in **Eq. 1** (Meng et al., 2018).

However, lightweight cryptography has been identified to overcome the extended hashing processes on the blockchain (Alfa et al., 2021a; Hassan et al., 2019). In addition, lightweight cryptographic schemes are generally weak but can be enhanced with hardening schemes such as Sooner (Alfa et al., 2021b). Authorizations and verifications of transactions on mined blocks in blockchain can be outsourced for effectiveness and speedups using AI approaches.

The process of reaching decisions about the mining of blocks and rewarding systems on blockchain technology can be effectively managed by AI approaches (Hassan et al., 2019). Ingenuine blocks are expected to be left unconfirmed and discarded by the blockchain networks in conjunction with Proof-of-Work and AI-inspired algorithms (Ensor et al., 2019). Blockchain technology can be superimposed on other technologies such as the Internet of Things to overcome problems of security, privacy, and delays (Hassan et al., 2019). The Byzantine general's problem can be resolved with blockchain in which reliability and transparency are introduced through an AI approach for effective data sharing among numerous end-users of the network (Atlam and Wills, 2019).

Transactions transmission, communication, and management in blockchain can be carried out more effectively through AI applications. The identity leakage problem and ineffective pseudo identities on the blockchain can be further protected through proof-of-conformance mechanisms using AI approaches such as computer vision (Yang and Yu, 2021). The linkability of identities to information kept on the blockchain has been ineffectively undertaken by anonymization of personally identifiable information (PII). Though, the secrecy of public-private keys of blockchain is the heart of its operational effectiveness, which can be achieved using AI schemes (Wirth and Kolain, 2018). There are numerous opportunities of integrating AI into blockchain technology by leveraging features such as decentralization, transparency, privacy, and auditability, for highly complex and intricate applications (Mukkamala et al., 2018).

The initial Blockchains were built on cryptographic primitives without trusting an entity for proofing rather than proofs derived from strong cryptography. The validation and endorsement of transactions rely entirely on digital signatures (Chatterjee and Chatterjee, 2017). However, new approaches based on AI such as pattern recognition could be explored. The virtualization of Distributed Ledger Technology (such as blockchain Technology) could overcome scalability and interoperability problems (Ensor et al., 2019). However, AI could play important roles in managing network traffic and the consummation of a large volume of transactions on blockchains.

Prospective Artificial Intelligence Solutions in Blockchain Technology

The prospects of AI in blockchain technology for overcoming perceived weaknesses from this study are summarized in **Table 1**.

AI IN BLOCKCHAIN TECHNOLOGY: CASES AND SCENARIOS

The AI has sufficient capabilities to advance the data exchanges and transmissions across cloud infrastructures through distributed and multi-computing, visualization, and large-scale computation. These enable numerous services to be performed in parallel including server, network hardware, and space maximization (Namasudra et al., 2020).

Big data applications require effective information extrapolation and conversion methods, which can be achieved through high-performance machine/deep learning algorithms. Again, the effectiveness of control access methods in big data applications can be improved with the use of malicious data/transaction identification based on deep learning schemes (Namasudra et al., 2020). Optimization approaches offered by machine learning searching and meta-heuristic algorithms in conjunction with decentralized database structures enable cloud service providers including Google's Cloud IoT, Microsoft's Azure IoT Edge, and Amazon's AWS Greengrass ().

Financial Chains and other decentralized applications (DAPPs) can be effectively scrutinized with deep learning algorithms to unveil malicious and ingenuine transactions and manipulations. Fake product reviews can be detected on Blockchain-based platforms using machine learning algorithms. Blockchain supports a secure platform for sharing digital content between buyers and sellers in which data risks can be minimized through machine learning techniques (Naz et al., 2019).

TABLE 1 | Prospects of AI in blockchain technology problems. Tick (√) indicates AI solution probable; tick (×) indicates AI solution improbable.

S/N	Blockchain technology weakness	AI solution applicable
1	Smart contracts	√
2	Authorization and verification	√
3	Complex cryptography and weak hashing functions	×
4	Mining decision-making process	√
5	Vulnerabilities to attacks and threats	√
6	Transactions delays	√
7	Byzantine generals' problem	√
8	Identity privacy and security leakages	√
9	Secrecy of public-private keys	√
10	Validation and endorsement of transactions	√
11	Network control and management	√
12	Scalability and interoperability	×
13	Data sharing ineffectiveness	√
14	Consensus mechanisms and protocols	√
15	Transparency and openness	×
16	Anonymization of PII	√

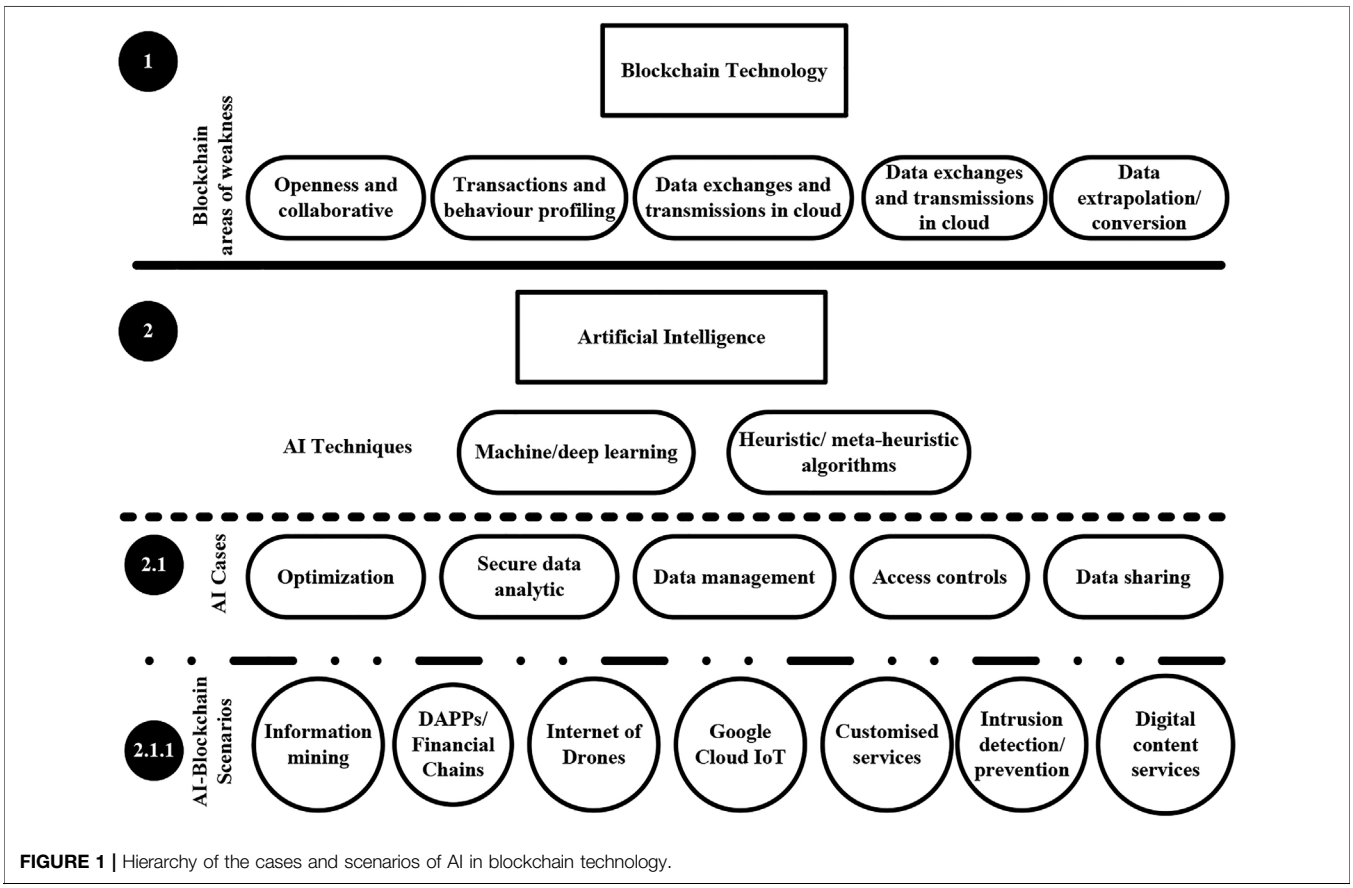

FIGURE 1 | Hierarchy of the cases and scenarios of AI in blockchain technology.

Blockchain-based drone monitoring system throughputs and network performance can be achieved through AI's deep learning to safeguard their routing and movement. The security of data collected and transmitted by drone airborne is jointly attained with Drone-based Delegated Proof of Stake and deep learning (Yazdinejad et al., 2020).

The collaborative and open mode of blockchain technology further raises the requirements for effectual data management. Therefore, machine learning and AI methods can be integrated into the blockchain to secure data analytics transparency (Faroukhi et al., 2020). The hierarchical representation of the main cases and scenarios of AI in blockchain technology is depicted in **Figure 1**.

CONCLUSION

The growth of blockchain technology can be viewed from three main perspectives in deriving values including the development of innovative models and far-reaching exploration; improved research on domain-specific and end-users; and the advancement of fresh enterprise capabilities. More so, there is the need to consider the adoption of formal models for the purpose of understanding the intricate complications and complexities surrounding the application of blockchain technology (Mukkamala et al., 2018).

The concept of smart contracts is similar to small pieces of software regulating a deal or transaction between a client and consumer, while it is dissimilar in the sense that the structure of financial smart contracts is different from that of non-financial smart contracts (Chatterjee and Chatterjee, 2017). Consequently, developers, security experts, and decentralized application programmers will need to collaborate effectively to move more quickly towards flawless blockchain-based applications through AI.

Blockchain technology is capable of offering Sensing-as-a-Service in which data from sensing objects are protected in exchange for certain incentives (Ensor et al., 2019). Then, AI could facilitate Sensing-as-a-Service platforms through the use of blockchain data in weather stations, smart precision farming, and other smart environments. The study contributed to the ongoing discussions on the use of AI to overcome problems of blockchain technology including network management, data exchanges, transaction verification, public-private keys management, smart contracts programming, the effectiveness of consensus protocols, and complex cryptography and weak hashing functions.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material; further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

The first author reviewed and modified the content of this manuscript. The second author wrote **Sections 1**, **2**, **4**, provided references, and formatted the manuscript. The third author wrote **Sections 3**, **5**, and **6**.

ACKNOWLEDGMENTS

The authors want to acknowledge their reviewers for their contributions in making this manuscript better and publishable.

REFERENCES

Abbasi, M. A., Memon, Z. A., Durrani, N. M., Haider, W., Laeeq, K., and Mallah, G. A. (2021). A Multi-Layer Trust-Based Middleware Framework for Handling Interoperability Issues in Heterogeneous IOTs. *Clust. Comput.* 24, 2133–2160. doi:10.1007/s10586-021-03243-1

Adenugba, F., Misra, S., Misra, S., Maskeliūnas, R., Damaševičius, R., and Kazanavičius, E. (2019). Smart Irrigation System for Environmental Sustainability in Africa: An Internet of Everything (IoE) Approach. *Math. Biosci. Eng.* 16 (5), 5490–5503. doi:10.3934/mbe.2019273

Al-Sulaiman, T., and Al-Matouq, A. (2021). A Convex Collaborative Filtering Framework for Global Market Return Prediction. *IEEE Access* 9, 29458–29469. doi:10.1109/access.2021.3058646

Alfa, A. A., Alhassan, J. K., Olaniyi, O. M., and Olalere, M. (2021). Blockchain Technology in IoT Systems: Current Trends, Methodology, Problems, Applications, and Future Directions. *J. Reliab. Intell. Environ.* 7 (2), 115–143. doi:10.1007/s40860-020-00116-z

Alfa, A. A., Alhassan, J. K., Olaniyi, O. M., and Olalere, M. (2021). "Sooner Lightweight Cryptosystem: Towards Privacy Preservation of Resource-Constrained Devices," in *ICTA 2020, CCIS*. Editors S. Misra and B. Muhammad-Bello (Midtown Manhattan, New York City: Springer International Publishing), 415–429. doi:10.1007/978-3-030-69143-1_32

Atlam, H. F., and Wills, G. B. (2019). Technical Aspects of Blockchain and IoT. *Adv. Comput.* 115, 1–39. doi:10.1016/bs.adcom.2018.10.006

Azzaoui, A. E., Singh, S. K., Pan, Y., and Park, J. H. (2020). Block5GIntell: Blockchain for AI-Enabled 5G Networks. *IEEE Access* 8, 145918–145935. doi:10.1109/ACCESS.2020.3014356

Battineni, G., Sagaro, G. G., and Chinatalapudi, N. (2020). Applications of Machine Learning Predictive Models in the Chronic Disease Diagnosis. *J. Pers. Med.* 10, 21. doi:10.3390/jpm10020021

Brandão, A., Mamede, H. S., and Gonçalves, R. (2018). Systematic Review of the Literature, Research on Blockchain Technology as Support to the Trust Model Proposed Applied to Smart Places. In: *Advances in Intelligent Systems and Computing*. Berlin/Heidelberg, Germany: Springer-Verlag p. 1163.

Cao, J., Zhang, Q., and Shi, W. (2018). Edge Computing: A Primer," in *SpringerBriefs in Computer Science*, Berlin/Heidelberg, Germany: Springer. doi:10.1007/978-3-030-02083-5_1

Chatterjee, R., and Chatterjee, R. (2017). "An Overview of the Emerging Technology: Blockchain," in Proceedings of the2017 International Conference on Computational Intelligence and Networks, CINE (IEEE), 126–127. doi:10.1109/cine.2017.33

Conti, M., Sandeep Kumar, E., Lal, C., and Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Commun. Surv. Tutorials* 20 (4), 3416–3452. doi:10.1109/comst.2018.2842460

Ensor, A., Schefer-Wenzl, S., and Miladinovic, I. (2019). "Blockchains for IoT Payments: A Survey," in 2018 IEEE Globecom Work GC Wkshps (IEEE).

Faroukhi, A. Z., El Alaoui, I., Gahi, Y., and Amine, A. (2020). A Multi-Layer Big Data Value Chain Approach for Security Issues. *Procedia Comput. Sci.* 175, 737–744. doi:10.1016/j.procs.2020.07.109

Feng, Q., He, D., Zeadally, S., Khan, M. K., and Kumar, N. (2019). A Survey on Privacy Protection in Blockchain System. *J. Netw. Comput. Appl.* 126, 45–58. doi:10.1016/j.jnca.2018.10.020

Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., and Janicke, H. (2018). Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet Things J.* 6, 2188–2204. doi:10.1109/JIOT.2018.2882794

Hassan, M. U., Rehmani, M. H., and Chen, J. (2019). Privacy Preservation in Blockchain Based IoT Systems: Integration Issues, Prospects, Challenges, and Future Research Directions. *Future Gener. Comput. Syst.* 97, 512–529. doi:10.1016/j.future.2019.02.060

Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., and Han, J. (2018). When Intrusion Detection Meets Blockchain Technology: A Review. *IEEE Access* 6, 10179–10188. doi:10.1109/access.2018.2799854

Mukkamala, R. R., Vatrapu, R., Ray, P. K., Sengupta, G., and Halder, S. (2018). Blockchain for Social Business: Principles and Applications. *IEEE Eng. Manag. Rev.* 46, 94–99. doi:10.1109/EMR.2018.2881149

Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., and Shanthini, A. (2020). Towards DNA Based Data Security in the Cloud Computing Environment. *Comput. Commun.* 151, 539–547. doi:10.1016/j.comcom.2019.12.041

Naz, M., Al-zahrani, F. A., Khalid, R., Javaid, N., Qamar, A. M., Afzal, M. K., et al. (2019). A Secure Data Sharing Platform Using Blockchain and Interplanetary File System. *Sustainability* 11 (7054), 1–24. doi:10.3390/su11247054

Salman, T., Zolanvari, M., Erbad, A., Jain, R., and Samaka, M. (2019). Security Services Using Blockchains: A State of the Art Survey. *IEEE Commun. Surv. Tutorials* 21 (1), 858–880. doi:10.1109/comst.2018.2863956

van Klompenburg, T., Kassahun, A., and Catal, C. (2020). Crop Yield Prediction Using Machine Learning: A Systematic Literature Review. *Comput. Electron. Agric.* 177, 105709. doi:10.1016/j.compag.2020.105709

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., and Wang, F-Y. (2019). Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man. Cybern. Syst.* 49, 2266–2277. doi:10.1109/tsmc.2019.2895123

Wang, D., Zhao, J., and Wang, Y. (2020). A Survey on Privacy Protection of Blockchain: The Technology and Application. *IEEE Access* 8, 108766–108781. doi:10.1109/access.2020.2994294

Wirth, C., and Kolain, M. (2018). "Privacy by BlockChain Design: A Blockchain-Enabled GDPR-Compliant Approach for Handling Personal Data," in ERCIM-Blockchain 2018: Blockchain Engineering - Challenges and Opportunities for Computer Science Research.

Yang, R., and Yu, Y. (2021). Artificial Convolutional Neural Network in Object Detection and Semantic Segmentation for Medical Imaging Analysis. *Front. Oncol.* 11, 1–9. doi:10.3389/fonc.2021.638182

Yang, Y., Yang, Y., Chen, J., and Liu, M. (2018). "Application of Blockchain in Internet of Things," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Berlin/Heidelberg, Germany: Springer-Verlag), 73–82. doi:10.1007/978-3-030-00018-9_7

Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Srivastava, G., and Aledhari, M. (2020). Enabling Drones in the Internet of Things with Decentralized Blockchain-Based Security. *IEEE Internet Things J.* 8 (8), 6406.

Zhang, M., Li, L., Wang, H., Liu, Y., Qin, H., and Zhao, W. (2019). Optimized Compression for Implementing Convolutional Neural Networks on FPGA. *Electronics* 8, 295. doi:10.3390/electronics8030295

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.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.