Proceedings of the 4th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/55/20241417

The integration of blockchain technology and artificial intelligence: Innovation, challenges, and future prospects

Yiwen Wang

School of Computer, Beijing Jiaotong University, Weihai, Shandong, 264402, China

1329595452@qq.com

Abstract. Blockchain provides a decentralised, tamper-proof and trustworthy distributed database technology that is widely used in finance and economics, IoT and big data. Artificial intelligence (AI) provides a technology that can mimic human intelligence, learn autonomously and automate decision-making, which plays a major role in enhancing productivity, solving complex problems and improving decision-making. The two represent two of the major driving forces in technology today, and their integration is redefining our digital world. The aim of this paper is to explore the integration of these two technologies and the innovations, challenges, and future prospects they bring. First, we trace their history and evolution, introduce the basic characteristics of blockchain and AI, and explain in detail how they work. We then delve into the integration of blockchain and AI, highlighting their importance and significance in areas such as finance, supply chain and healthcare. We analyse the applications and implications of this integration for these areas, as well as the challenges and dilemmas faced, including issues of security, privacy, data leakage, and technical feasibility. Finally, we explore future trends and related work, highlighting the importance of global community collaboration and innovation to realize the potential of blockchain and AI.

Keywords: Blockchain, Artificial Intelligence, Integration.

1. Introduction

1.1. The Rise of Blockchain

After the innovation of digital cryptocurrencies in 2008, the distributed accounting method and decentralized solution of blockchain technology gained more and more attention from scientists and researchers. Bitcoin became the first cryptocurrency not controlled by a single entity and the first successful blockchain application, and grew rapidly within a few years, attracting investment from all types of companies and government involvement [1].

Bitcoin proposes a protocol that allows users to exchange currencies with each other with limited resources. In the case of Bitcoin, limited resources are an objective constraint on solving mathematical computational difficulties, and are not limited to that [2]. Bitcoin has been an enlightening and huge boost to blockchain technology, and the blockchain ecosystem has been formed thanks to Ether, whose launch has opened up new avenues for the development of smart contracts, allowing developers to create a variety of blockchain-based applications [3].

DOI: 10.54254/2755-2721/55/20241417

1.2. The Evolution of Artificial Intelligence

The development of artificial intelligence began around 1950. This period can be summarized as the Symbolist era, when research focused on rule-based and expert systems, aiming to represent knowledge and problem-solving in symbols [4]. According to the conclusion by Delipetrev, 1960-1980 is called the Connectionist era, which saw the emergence of a number of computational models based on mimicking the neural system but was followed by a cold AI winter due to a lack of computational resources and theoretical problems.

From 1980-1990, AI development entered the era of expert systems, which used expert knowledge bases and rules to solve domain-specific problems such as medical diagnosis and financial analysis. However, the limitations of expert systems and the problem of maintaining the knowledge base restricted their further development [5].

Since 1990, the rise and rapid development of statistical, machine and deep learning has led to tremendous progress and achievements in the field of AI.Deep learning has seen tremendous breakthroughs, including major advances in areas such as image recognition, speech recognition, natural language processing, and reinforcement learning. Deep learning models such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have improved the performance of many AI applications [6].

1.3. The Importance of Blockchain and AI

The importance of the combined application of blockchain and AI is that they complement each other and work together to create more secure, trustworthy and efficient solutions. This combination offers a wide range of opportunities for data security and privacy, smart contracts, transparency and decentralised innovation that promise to have a profound impact across industries.

1.3.1. Data Security and Privacy Protection

The advancement of technology has changed the search for new technologies, the market for Unmanned Aerial Vehicles (UAVs) is expanding, and the issues of data security and privacy protection are increasing. Blockchain technology is very effective, and the proposed privacy protection scheme encrypts the data using the cryptosystem data of the Number Theory Research Unit and provides privacy analysis to verify the security requirements. In addition, the protection scheme has low computational cost in key generation, encryption and decryption [7].

Clearly, that's why blockchain is important in terms of data security and privacy protection, and its functionality can be further enhanced by adding AI for data training and decision-making [8]. Based on Rajawat's research, the decentralized nature of blockchain makes it ideal for data security. While traditional centralized data storage makes data vulnerable to hacking and misuse, blockchain offers a higher level of data security protection through distributed ledgers and encryption. Artificial intelligence requires large amounts of data for training and decision-making. Combining AI with blockchain can ensure that the privacy of sensitive data is protected, allowing users to trust AI systems more and use them in more application scenarios, such as in medicine and healthcare.

1.3.2. Smart Contract

Smart contracts on the blockchain are self-executing contracts that do not require an intermediary. By combining AI with smart contracts, more complex and intelligent automated processes can be created. For example, insurance claims can be automatically verified by AI, and payments can be made based on data on the blockchain without human intervention. This combination can increase the efficiency of contract enforcement and reduce the costs and delays associated with traditional legal processes.

1.3.3. Decentralized Application

Data silos and computational resource constraints in centralized AI architectures increase their technical barriers, thus, distributed AI collaboration in terms of data, models and resources has attracted intensive research interest. Liwei Ouyang proposes a framework for writing Learning Marketplaces (LMs), where

DOI: 10.54254/2755-2721/55/20241417

the blockchain provides a de-trusted environment for collaboration and transactions, and the smart contract serves as a software-defined agent to encapsulate and handle scalable collaborative relationships and market mechanisms [9].

The combination of blockchain and AI helps create decentralized applications that are not controlled by a single entity. This is essential for delivering more open, democratic and innovative solutions. For example, decentralized AI marketplaces can allow developers to share and exchange AI models without having to go through an intermediary platform. This decentralized approach can help lower barriers to innovation and facilitate technological progress.

1.4. Purpose and Importance of the Study

The study aims to analyse the synergies between blockchain technology and artificial intelligence in order to create more powerful and intelligent solutions. This includes exploring the complementary and mutually reinforcing nature of the two, and how they can work together to address real-world challenges. The primary purpose of the research is to identify and analyse the innovations that integration brings. By delving into case studies and successful implementations, the study aims to reveal the nature of the innovation and the changes it has brought about. The study will also discuss the challenges and issues associated with integration. These include data security and privacy issues, technical difficulties, legal and regulatory challenges, and socio-ethical considerations. These issues will be explored in depth and possible solutions proposed.

Finally, our research will consider future trends in the integration of blockchain technology and AI, exploring possible research directions and emerging areas, as well as their potential impact on technology, business and society. A comprehensive understanding of the integration of blockchain technology and AI, highlighting its innovative potential, challenges and future prospects, is the most significant part of this thesis.

2. Blockchain and Artificial Intelligence

2.1. Blockchain Technology Fundamentals: Working Principle

Blockchain works on the principle of a distributed ledger technology that allows multiple participants to conduct transactions in a decentralized environment with a consensus mechanism to ensure the security and trustworthiness of the data.

2.1.1. The Structure of Blockchain

The figure created by Gad below (Figure 1.) shows a large blockchain instance consisting of a block header (80 bytes long), which includes metadata such as the block version (4 bytes), the Merkle tree root hash (32 bytes), the timestamp (4 bytes), the bits (4 bytes), the nonce (4 bytes), and the parent block hash (32 bytes), as well as the block body [10].

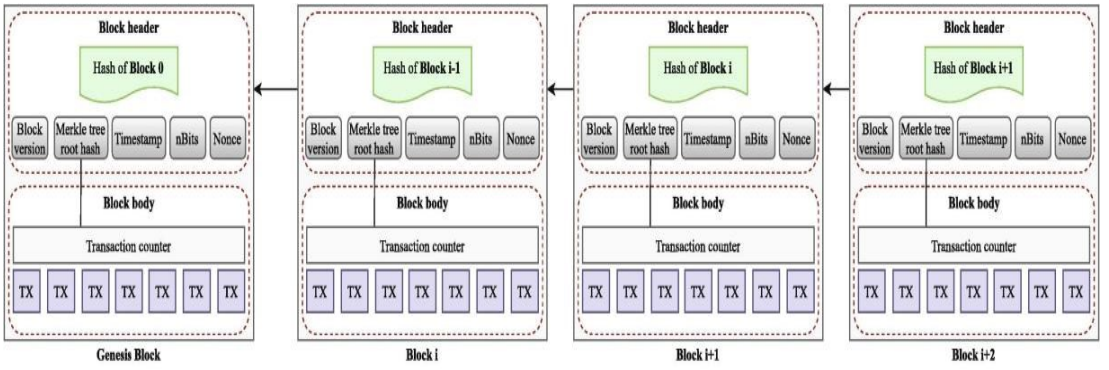

Figure 1. Blockchain Instance

DOI: 10.54254/2755-2721/55/20241417

According to Zeng, the structure of a blockchain is a distributed, growing data structure consisting of a series of blocks, each containing multiple transactions or records [11]. When building a blockchain, there is first an initial block, often referred to as the 'genesis block'. Each new block is then connected to the previous block in chronological order. Blockchain users participate in building the blockchain through a process called 'mining', which is the process of finding a solution that corresponds to a particular hash value. When a user finds a solution, they broadcast it across the network. Other users verify the solution to ensure it is valid. This process is repeated over and over again, and the entire blockchain is built. Eventually, the blockchain contains all transactions and records, with a growing chain structure. This process ensures the security and trustworthiness of the data, and the decentralization and consensus mechanisms of the blockchain make it a secure and reliable distributed data management system.

2.1.2. The Characters of Blockchain

Based on Islam's analysis and summary of blockchain technology, the retrieved attributes are classified into three clusters through affinity diagrams, as shown in Table 1 [12].

Table 1. Concepts of Blockchain

Ser	Concept	Relation	Concept	Relation	Concept
1	Blockchain	includes	Service Perspective	which offers	Scalability
2				which has	Validation
3				which offers	Multiple Writers
4				which has	Distributed Trust
5		supports	Logical Inclusion	which provides	Computational Logic
6				which has	Transaction Dependency
7				which offers	Transaction Rules
8		includes	Architectural Characteristics	which have	Shared Database
9				which use	P2P Transmission
10				which comprehend	Disintermediation
11				which have	Timestamped Blocks
12				which include	Immutable Records
13				which has	Encrypted Data Transmission

The table shows attributes and features very clearly. Clustering is a service perspective, logical containment and architectural features. Blockchain has attributes such as scalability, authentication, multiple writers, and distributed trust, which means it is capable of handling large numbers of transactions, ensures the legitimacy of transactions, allows multiple participants to write data, and does not need to rely on a central authority. Logic includes attributes such as computational logic, transaction dependencies and transaction rules. Data and transactions on the blockchain are subject to complex computational logic and rules, with dependencies between transactions. Architectural features include a shared database, P2P transmission, disintermediation, timestamped blocks, immutable records and encrypted data transmission. These features contribute to the security, reliability and privacy of the blockchain, making it a robust distributed system.

2.1.3. Working Model of Blockchain

Blockchain is a distributed ledger technology with a working model based on distributed networks, consensus algorithms and cryptography. As summarized by Bhushan, the overall working model is

DOI: 10.54254/2755-2721/55/20241417

complex but organised, and according to this paper, we will not explain it too much, but only roughly sort out the working process to facilitate the reader's understanding [13].

1. Distributed network: The blockchain network consists of multiple nodes that are distributed across the globe with no central controlling authority. Each node contains a complete copy of the blockchain, which means that data is stored in multiple locations rather than being centralised on a single central server.

2. Transaction broadcasting: The created transaction is broadcasted to multiple nodes in the blockchain network. These nodes propagate the transaction information through peer-to-peer communication, making all nodes aware of the new transaction.

3. Consensus mechanisms: Nodes in a blockchain network need to reach a consensus to determine which node has the right to add a new block to the chain. Common consensus algorithms include Proof of Work (PoW) and Proof of Stake (PoS). These mechanisms ensure the security of the network against attacks by malicious nodes.

4. Encryption and digital signatures: Blockchain uses encryption to protect the security and privacy of data. Each transaction is digitally signed to verify the identity of the sender, while a hash function is used to protect the integrity of the data.

The transaction data on the blockchain and the successive addition of blocks form a growing chain structure that ensures the security and integrity of the data. Blockchain's decentralized nature and consensus mechanism make it a powerful distributed system for a wide range of applications.

2.2. Artificial Intelligence Fundamentals

2.2.1. Definition of AI

Drawing on Ballester's work and a summary of evidence from various sources, I will define this from different perspectives. From the perspective of modelling human intelligence, AI aims to simulate and replicate the ability of human intelligence to act and think, including learning, reasoning, problem-solving, perception and decision-making. From a task automation perspective, AI is a technology that aims to improve efficiency and accuracy by automating tasks and processes without human intervention [14]. From an auto-learning perspective, AI is a system that is capable of learning and improving itself automatically, continuously improving its performance based on experience and data without the need for explicit programming. From an intelligent agent perspective, AI is a type of intelligent agent that can sense its environment and make adaptive decisions based on changes in the environment to achieve specific goals.

2.2.2. Classification of AI

Artificial Intelligence covers a wide range of fields and requires different values in different industries and domains, so there is no limit to the way it can be categorized.

Based on Flowers' research, it is possible to distinguish between weak and strong AI. Weak AI are AI systems that focus on solving specific tasks or domains. These systems exhibit high levels of intelligence in a limited number of domains but perform poorly in others, such as voice assistants (Siri) and image recognition systems [15]. Strong AI, on the other hand, are systems that have intelligence and cognitive capabilities similar to human intelligence. Such systems are not only capable of performing specific tasks but also have the ability to learn, understand, reason and adapt [15].

Machine Learning (ML) is a branch of AI that enables computer systems to learn and improve from data without the need for explicit programming and includes techniques, such as natural language processing, image recognition, recommender systems, etc. [16]. Miric's survey also shows that Deep Learning (DL), a branch of Machine Learning, uses neural networks to simulate the structure of the human brain to process large and complex data. It has already achieved significant results in areas such as image and speech recognition, including CNNs and RNNs.

The category of perception and machine vision is also a very important area of research at the moment. Engel's survey states that this enables machines to perceive and understand their surroundings and the

DOI: 10.54254/2755-2721/55/20241417

environment in the moment. It currently plays an important role in face recognition and visual perception in self-driving cars [17].

3. Innovation and Application

Blockchain and Artificial Intelligence are widely used in the innovation space, and their combination brings new opportunities and solutions to many industries. Together, they are driving innovation and efficiency, providing powerful tools and methods for future growth and solving complex problems.

3.1. Financial Industry

To quote Sharma, technology has transformed the industrial age into the silicon age, thus creating fintech [18]. Apart from the earliest Bitcoin, blockchain technology has demonstrated various applications and capabilities in the financial services sector.

Blockchain's smart contracts can be combined with AI technology to automate the execution of financial transactions and contracts so that they can be executed automatically based on predefined conditions, reducing the need for human intervention. The combination of AI and blockchain can improve and personalise the customer service experience. Next, this paper will make specific statements in several different sections.

3.1.1. Mobile Payments and Cryptocurrency

Xu and Gao point out that the penetration of smart devices is increasing dramatically, which is also causing mobile payments to gradually transform into the main payment method in life and production. Blockchain-based cryptocurrencies are becoming an extremely important type of currency, so supporting cryptocurrency payments on mobile devices is becoming a necessary requirement [19].

Hosen evaluates the uses and benefits of integrating AI and blockchain platforms on many financial services platforms, and we can get an idea of the huge impact of decentralised cryptocurrencies on the financial sector [20].

AI can provide smart payment suggestions and optimise payment processes. This makes mobile payments more convenient and personalised, while reducing manual operations. Also, it can ensure secure and convenient payments for digital currencies. Smart contracts can be used to automate digital currency transactions, increasing payment efficiency. AI can monitor transactions on payment platforms to identify potential fraud and improve the security of payments. Blockchain's tamperability helps ensure the integrity of transaction records, providing an additional layer of protection.

3.1.2. Stock Market

As Mosteanu says, in an era of digitization and intelligence, machines will solve a large number of repetitive, time-consuming and tedious tasks, giving financiers more time for higher-level, more profitable analysis and research [21]. In the stock market, the combination of AI and blockchain has transformed the way stocks are analyzed and asset managed. While improving the efficiency and transparency of the market, investors and exchanges enjoy a wider range of tools and services.

AI and blockchain combined can improve asset management strategies. Smart contracts can automate asset allocation and portfolio management, adjusting to market conditions, which helps investors optimise their portfolios and improve the efficiency of asset management. Blockchain technology supports decentralised exchanges, allowing investors to trade digital assets without relying on traditional intermediaries. This provides more trading options and financial inclusion. Meanwhile AI can be used to monitor the activities of decentralised exchanges, detecting potential anomalies and making activities more secure.

3.1.3. Decentralized Finance (DeFi)

DeFi is a financial service and application based on blockchain technology and smart contracts. Featuring decentralization, openness, transparency, automation, and diversity, DeFi aims to change the way the traditional financial system works by providing users with more financial freedom and choice

DOI: 10.54254/2755-2721/55/20241417

[22]. According to Huynh-The's research, the combination of AI and blockchain has had a profound impact on the DeFi space, driving the decentralization and digitalisation of financial services. It has improved the efficiency, security and trustworthiness of the DeFi platform while also providing users with more financial tools and financial inclusion.

AI can be used to develop more sophisticated and intelligent DeFi smart contracts that can automatically execute complex financial transactions and strategies based on market conditions. At the same time, the use of blockchain technology can ensure that smart contracts are transparent and tamper-proof, making DeFi trading more secure and trustworthy. Smart contracts can automatically balance asset portfolios to provide optimal liquidity provision strategies. Blockchain supports Decentralized Exchanges (DEX) and AI can be used to enhance the user experience of DEX, including price prediction, trade recommendations and user interface improvements.

3.2. Supply Chain Management

The combination of AI and blockchain increases supply chain visibility, trust, and efficiency, reducing fraud and errors, while also providing supply chain parties with more data and tools to improve their operations and decision-making.

1. The quality of supply can be effectively controlled. Blockchain can record production and quality inspection data of products to ensure quality and compliance, and then use smart contracts to automatically execute payments or quality issues based on quality standards. AI can reduce the production of defective products by analysing product quality data to identify potential quality issues in advance. Aliahmadi's research sheds light on this issue, reflecting the Internet of Things (IoT), Artificial Intelligence (AI) and Blockchain, among other technologies, can bring a lot of benefits to security in a smart supply chain [23].

2. According to Wamba's survey, blockchain can be used to record and track the movement of goods in the logistics process, providing more comprehensive supply chain visibility [24]. Smart contracts can automatically track the status and location of goods, giving all parties in the supply chain real-time visibility into the location and status of goods. AI can use this blockchain data to predict the impact of traffic, weather, or other factors on logistics and provide real-time updates, offering more accurate supply chain forecasting and planning for improved delivery time estimates.

3.3. Healthcare

Healthcare is being digitized, electronic health records are becoming more common, smart health is becoming popular, and the healthcare system can be significantly improved using AI and blockchain technology. Blockchain emerges as a potentially revolutionary option for enhancing data management and security in healthcare systems, effectively addressing the threat of data breaches and malicious attacks on smart healthcare. Based on Soltanisehat's approximately five years of statistics and surveys on the impact of technology in healthcare, we can conclude that the combination of AI and blockchain has the potential for a wide range of applications in the healthcare sector, from patient data management to drug supply chain traceability, to improve the efficiency, transparency and security of the healthcare system [25]. This combination is important for providing better healthcare services, improving disease prevention and treatment, and reducing healthcare costs.

1. Haddad's study states that traditional EHR systems are usually managed by healthcare organisations, which have data security and privacy issues. Whereas Electronic Health Records (EHRs) are digitally stored health records that are usually shared among healthcare stakeholders and are therefore vulnerable to issues such as power failures, data misuse, and lack of privacy, blockchain technology can be an effective solution to this problem. However, scalability and complexity issues may make it inefficient, and the inclusion of artificial intelligence algorithms becomes particularly important [26].

2. Blockchain provides a secure way to share medical data, for example, between different healthcare providers or between patients and their doctors, where patients can control access to their medical data.AI algorithms can use the shared data to conduct medical research and trend analyses to improve

DOI: 10.54254/2755-2721/55/20241417

disease diagnosis and treatment. In addition to this, as mentioned in Anoop's paper, blockchain and AI can be used to monitor patient health data such as vital signs, medical records and exercise data [27]. All these can help in realising a credible healthcare ecosystem.

4. Challenges and Problems

The combination of blockchain and AI represents an exciting technology trend, and privacy and data security issues, technical issues, performance issues, and smart contract vulnerabilities all need to be carefully considered and addressed in realizing this combination.

4.1. Security and Privacy Issues

Blockchain ensures that data is transparent and untamperable, but this also makes data stored on the blockchain visible to all participants. For AI applications that contain sensitive information, this can raise privacy concerns. For example, in the case of autonomous vehicles (AVs), which are rapidly evolving, as mentioned by Bendiab, the combination of blockchain and AI opens up new opportunities for hackers to carry out malicious attacks, seriously threatening the future of mobility and data protection [28].

Common techniques such as zero-knowledge proofs and homomorphic encryption can enable privacy protection on the blockchain while allowing AI to analyse encrypted data. For example, the ZeeStar language proposed by Steffen better handles such private issues as data privacy [29]. However, the increase in computational processes directly affects the efficiency of the system, so the rational use of AI algorithms to improve efficiency still requires continued research.

4.2. Technical Challenges

In the combination of blockchain and AI, it is crucial to ensure the relevance and consistency of on-chain data and off-chain data. Because under the premise of ensuring data integrity, we must achieve an effective combination of blockchain systems and traditional information systems. Artificial intelligence algorithms are closely related to data, but AI technology still faces many problems, such as poor data quality, data monopoly, and data misuse. The combination with blockchain provides new challenges and new opportunities.

Kumari's proposed Energy Cloud Management (ECM) system exposes this problem very appropriately. In order to integrate energy infrastructure with smart energy usage and value-added services based on consumer demand, the two main technical issues of efficient demand-side forecasting and secure data transfer are the most prominent, especially the data-related algorithms and techniques, and also the very open challenges in the process of combining blockchain and AI [30].

4.3. Scalability

Blockchain's performance issues, such as transaction speed and processing power, may limit its application in combination with AI. AI requires significant computational resources, which may lead to inefficiencies in applications combined with blockchain. Similar to most application technologies, scalability issues are a key focus for the successful implementation of applications. Many blockchain companies and platforms are also actively working to improve their performance and scalability.

For example, Samuel proposed an Improved Sparse Neural Network (ISNN) that was tested for scalability by increasing the number of consumer-producers, which was ultimately applied to a residential trading system [31].

In Belhadi's research, an end-to-end intelligence framework developed to train medical data for Internet of Medical Things (IoMT) scenarios utilizes exactly blockchain technology. And the results show that strong performance can be achieved in a compressed epoch count with high learning rates and small batches. This also shows that the use of segmentation is an effective way to improve scalability and performance [32].

DOI: 10.54254/2755-2721/55/20241417

4.4. Smart Contract Vulnerability

In 2016, an attack on a smart contract called "The DAO" on Ether led to the theft of more than $30 million in cryptocurrency, and in 2017, a vulnerability in the smart contract of Parity's multi-signature wallet led to the freezing of about 150,000 Ether coins, making them inaccessible. All of these cases occurred due to smart contract vulnerabilities.

Smart contracts are automated code on the blockchain, but they are also vulnerable to vulnerabilities and attacks. Smart contract vulnerabilities can lead to financial losses and data breaches, so this is a huge challenge in the development of the combination of blockchain and AI. There are many ways to detect, prevent, and avoid these risks. Liao proposed SoliAudit (Solidity Audit), which employs machine learning techniques to validate 13 vulnerabilities using Solidity code as a learning function [33]. Zhang proposed a new hybrid deep learning model called CBGRU, which uses different models to extract features and consider these features for smart contract vulnerability detection [34].

5. Prospects

5.1. Future Trends in Blockchain and AI

The mutual integration of blockchain and artificial intelligence represents a key trend in the future of technology that will create a wave of revolutionary change in several areas. In the future, we can expect to see the rise of decentralized AI, booming data sharing and marketplaces, further upgrading of smart contracts, and a wide range of applications in areas such as supply chain management, finance, and healthcare.

Internet of Things (IoT) networks are growing rapidly and their security is becoming increasingly problematic. IoT networks need a scalable, decentralised and adaptive defence system, and it is clear that solutions integrated with blockchain and AI will play a huge role in the future. Table 2. shows the different forms of cybersecurity attacks in the IoT, which can also reflect the importance of blockchain and AI. The future is bound to design a perfect model to train data that can allow the existence of blockchain and protect the privacy of all IoT participants.

The convergence of AI and blockchain will create new business models through digitization. Artificial Intelligence and Blockchain are key technologies driving the wave of digital transformation. The convergence of these two technologies can improve current business practices and introduce new business models that can make autonomous decisions as independent economic agents.

5.2. Future Work

1. Ensuring the relevance and consistency of on-chain data and off-chain data has always been a key issue, and for different scenarios and application areas, future research in this area will definitely need to continue to develop.

2. Privacy and security issues gradually continue to arise with the development of technology, so research on privacy protection technology to improve the security of smart contracts and blockchain protocols to prevent attacks and vulnerabilities is also a major task in the future.

3. In order to improve performance and expandability, it is necessary to continue to study programming languages and tools for smart contracts in depth and to explore more and more advanced automated testing and verification methods for smart contracts in order to improve their development efficiency and reliability.

4. Blockchain is developing too fast, which also means that society is bound to have a relative lag in the introduction of relevant industry regulations, so chaos and bubbles will inevitably occur. This requires that we need to strengthen the efforts to raise user awareness and the laws and regulations related to it.

DOI: 10.54254/2755-2721/55/20241417

Table 2. Cybersecurity Attacks

Type	Action	LoT Layer	Effect
End Device Attacks	Attacker owns the physical control of LoT devices.	Perception Layer	Attacker can access confidential data such as keys and certificates. Further, the attacker may use the stolen confidential data to pretend to be an authentic node.
Communication Channel Attacks	Attacker intercepts the communication of the unencrypted channels to gain access to the confidential data.	Network Layer	Disclosure of LoT data.
Network Protocol Attacks	Attacker exploits the vulnerabilities of the used network protocol to launch different attacks such as blackhole attacks, DDoS attacks.	Network Layer & Application Layer	The efficiency and precision of the LoT network would be degraded by this type of attack.
Sensory Data Attacks	Attacker alters and tampers the data before they reach the destination.	Network Layer & Application Layer	Corrupted data will be spread across the LoT network.
DoS Attack	Attacker depletes the LoT resources by sending a huge number of fake requests to make LoT services unavailable to authorized users.	Network Layer & Application Layer	The LoT resources will be completely consumed, and the whole network will be overwhelmed.
Software Attacks	Attacker exploits the software vulnerabilities to own full control of software using viruses and worms.	Application Layer	Attacker uses these types of attacks to perform advanced attacks such as the DoS attack.

6. Conclusion

The integration of blockchain and artificial intelligence marks the dawn of a new technological era, and their joint application will spark tremendous innovation and change on a global scale. By combining decentralised and trusted data records with automated and intelligent decision-making systems, we will usher in a more efficient, secure, and reliable digital world. Despite the challenges, such as data security and privacy issues, scalability conundrums, and smart contract vulnerabilities, these challenges also inspire continuous improvement and innovation. We need to actively collaborate across the boundaries of academia, industry, and government sectors to develop appropriate regulations and standards to ensure the sustainable development of blockchain and AI integration.

In the future, we can expect to see more exciting use cases across finance, supply chain, healthcare, education and energy. This will bring positive changes to society and the economy, increasing efficiency, reducing costs and improving quality of life. As technology continues to evolve, the future trends of blockchain and AI will continue to drive us toward a smarter, more connected and secure future. Therefore, we should continue our commitment to research and innovation to address future challenges and explore more opportunities to realize the potential of blockchain and AI integration.

References

[1] Beck, R. (2018). Beyond bitcoin: The rise of blockchain world. Computer, 51(2), 54–58. https://doi.org/10.1109/mc.2018.1451660

DOI: 10.54254/2755-2721/55/20241417

[2] Martínez, V. G., Hernández-Álvarez, L., & Encinas, L. H. (2020). Analysis of the cryptographic tools for blockchain and bitcoin. Mathematics, 8(1), 131. https://doi.org/10.3390/math8010131

[3] Vujicic, D., Jagodic, D., & Randic, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH). http://dx.doi.org/10.1109/infoteh.2018.8345547

[4] Delipetrev, B. (2020, January 1). Historical evolution of artificial intelligence. UGD Academic Repository. https://eprints.ugd.edu.mk/28050/

[5] Brock, D. C. (2018). Learning from artificial intelligence's previous awakenings: The history of expert systems. AI Magazine, 39(3), 3–15. https://doi.org/10.1609/aimag.v39i3.2809

[6] Cohen, S. (2021). The evolution of machine learning: Past, present, and future. In Artificial Intelligence and Deep Learning in Pathology (pp. 1–12). Elsevier. http://dx.doi.org/10.1016/b978-0-323-67538-3.00001-4

[7] Lv, Z., Qiao, L., Hossain, M. S., & Choi, B. J. (2021). Analysis of using blockchain to protect the privacy of drone big data. IEEE Network, 35(1), 44–49. https://doi.org/10.1109/mnet.011.2000154

[8] Rajawat, A. S., Bedi, P., Goyal, S. B., Shaw, R. N., Ghosh, A., & Aggarwal, S. (2022). AI and blockchain for healthcare data security in smart cities. In AI and IoT for Smart City Applications (pp. 185–198). Springer Nature Singapore. http://dx.doi.org/10.1007/978-981-16-7498-3_12

[9] Ouyang, L., Yuan, Y., & Wang, F.-Y. (2022). Learning markets: An AI collaboration framework based on blockchain and smart contracts. IEEE Internet of Things Journal, 9(16), 14273–14286. https://doi.org/10.1109/jiot.2020.3032706

[10] Gad, A. G., Mosa, D. T., Abualigah, L., & Abohany, A. A. (2022). Emerging trends in blockchain technology and applications: A review and outlook. Journal of King Saud University - Computer and Information Sciences, 34(9), 6719–6742. https://doi.org/10.1016/j.jksuci.2022.03.007

[11] Zeng, Z., Li, Y., Cao, Y., Zhao, Y., Zhong, J., Sidorov, D., & Zeng, X. (2020). Blockchain technology for information security of the energy internet: Fundamentals, features, strategy and application. Energies, 13(4), 881. https://doi.org/10.3390/en13040881

[12] Islam, I., Munim, K. Md., Oishwee, S. J., Islam, A. K. M. N., & Islam, M. N. (2020). A critical review of concepts, benefits, and pitfalls of blockchain technology using concept map. IEEE Access, 8, 68333–68341. https://doi.org/10.1109/access.2020.2985647

[13] Bhushan, B., Sahoo, C., Sinha, P., & Khamparia, A. (2020). Unification of Blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions. Wireless Networks, 27(1), 55–90. https://doi.org/10.1007/s11276-020-02445-6

[14] Ballester, O. (2021, June 9). An artificial intelligence definition and classification framework for public sector applications. DG.O2021: The 22nd Annual International Conference on Digital Government Research. http://dx.doi.org/10.1145/3463677.3463709

[15] Flowers, J. C. (n.d.). Strong and Weak AI: Deweyan Considerations. https://ceur-ws.org/Vol-2287/paper34.pdf

[16] Miric, M., Jia, N., & Huang, K. G. (2022). Using supervised machine learning for large-scale classification in management research: The case for identifying artificial intelligence patents. Strategic Management Journal, 44(2), 491–519. https://doi.org/10.1002/smj.3441

[17] Engel, D., & Curio, C. (2011, June). Pedestrian detectability: Predicting human perception performance with machine vision. 2011 IEEE Intelligent Vehicles Symposium (IV). http://dx.doi.org/10.1109/ivs.2011.5940445

[18] Sharma, J. (1 C.E., January 1). Blockchain technology adoption in financial services: Opportunities and challenges. IGI Global. https://www.igi-global.com/chapter/blockchain-technology-adoption-in-financial-services/326987

DOI: 10.54254/2755-2721/55/20241417

[19] Xu, L., Chen, L., Gao, Z., Carranco, L., Fan, X., Shah, N., Diallo, N., & Shi, W. (2020). Supporting blockchain-based cryptocurrency mobile payment with smart devices. IEEE Consumer Electronics Magazine, 9(2), 26–33. https://doi.org/10.1109/mce.2019.2953734

[20] Hosen, M., Thaker, H. M. T., Subramaniam, V., Eaw, H.-C., & Cham, T.-H. (2023). Artificial intelligence (AI), blockchain, and cryptocurrency in finance: Current scenario and future direction. In Lecture Notes in Networks and Systems (pp. 322–332). Springer International Publishing. http://dx.doi.org/10.1007/978-3-031-25274-7_26

[21] An, Y. J., Choi, P. M. S., & Huang, S. H. (2021). Blockchain, cryptocurrency, and artificial intelligence in finance. In Fintech with Artificial Intelligence, Big Data, and Blockchain (pp. 1–34). Springer Singapore. http://dx.doi.org/10.1007/978-981-33-6137-9_1

[22] Banaeian Far, S., Imani Rad, A., & Rajabzadeh Asaar, M. (2023). Blockchain and its derived technologies shape the future generation of digital businesses: A focus on decentralized finance and the Metaverse. Data Science and Management, 6(3), 183–197. https://doi.org/10.1016/j.dsm.2023.06.002

[23] Aliahmadi, A., & Nozari, H. (2022). Evaluation of security metrics in AIoT and blockchain-based supply chain by Neutrosophic decision-making method. Supply Chain Forum: An International Journal, 24(1), 31–42. https://doi.org/10.1080/16258312.2022.2101898

[24] Wamba, S. F., & Queiroz, M. M. (2020). Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. International Journal of Information Management, 52, 102064. https://doi.org/10.1016/j.ijinfomgt.2019.102064

[25] Vyas, S., Shabaz, M., Pandit, P., Parvathy, L. R., & Ofori, I. (2022). Integration of artificial intelligence and blockchain technology in healthcare and agriculture. Journal of Food Quality, 2022, 1–11. https://doi.org/10.1155/2022/4228448

[26] Haddad, A., Habaebi, M. H., Islam, Md. R., Hasbullah, N. F., & Zabidi, S. A. (2022). Systematic review on ai-blockchain based e-healthcare records management systems. IEEE Access, 10, 94583–94615. https://doi.org/10.1109/access.2022.3201878

[27] Anoop, V. S., & Asharaf, S. (2022). Integrating artificial intelligence and blockchain for enabling a trusted ecosystem for healthcare sector. In Intelligent Healthcare (pp. 281–295). Springer Nature Singapore. http://dx.doi.org/10.1007/978-981-16-8150-9_13

[28] Patel , V., & Shah, M. (2022). Artificial intelligence and machine learning in drug discovery and development. Intelligent Medicine, 2(3), 134–140. https://doi.org/10.1016/j.imed.2021.10.001

[29] Steffen, S., Bichsel, B., Baumgartner, R., & Vechev, M. (2022, May). ZeeStar: Private smart contracts by homomorphic encryption and zero-knowledge proofs. 2022 IEEE Symposium on Security and Privacy (SP). http://dx.doi.org/10.1109/sp46214.2022.9833732

[30] Kumari, A., Gupta, R., Tanwar, S., & Kumar, N. (2020). Blockchain and AI amalgamation for nergy cloud management: Challenges, solutions, and future directions. Journal of Parallel and Distributed Computing, 143, 148–166. https://doi.org/10.1016/j.jpdc.2020.05.004

[31] Samuel, O., Javaid, N., Alghamdi, T. A., & Kumar, N. (2022). Towards sustainable smart cities: A secure and scalable trading system for residential homes using blockchain and artificial intelligence. Sustainable Cities and Society, 76, 103371. https://doi.org/10.1016/j.scs.2021.103371

[32] Belhadi, A., Holland, J.-O., Yazidi, A., Srivastava, G., Lin, J. C.-W., & Djenouri, Y. (2023). BIoMT-ISeg: Blockchain internet of medical things for intelligent segmentation. Frontiers in Physiology, 13. https://doi.org/10.3389/fphys.2022.1097204

[33] Liao, J.-W., Tsai, T.-T., He, C.-K., & Tien, C.-W. (2019, October). SoliAudit: Smart contract vulnerability assessment based on machine learning and fuzz testing. 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS). http://dx.doi.org/10.1109/iotsms48152.2019.8939256

[34] Zhang, L., Chen, W., Wang, W., Jin, Z., Zhao, C., Cai, Z., & Chen, H. (2022). CBGRU: A detection method of smart contract vulnerability based on a hybrid model. Sensors, 22(9). https://doi.org/10.3390/s22093577