International Journal of Intelligence Multidisciplinary Engineering Research(IJIMER) Con. Vol1: Aug 2024, pp: 05-09.
ISSN: 2583-9160

Conference Proceedings

Integrating Blockchain and Artificial Intelligence: A Review

Sivapriya Venkateswarar,[1], U. Padmavathi[2]
[1]UG student, Department of Computer Science and Engineering, Shiv Nadar University, Chennai, India.
[2]Assistant Professor, Department of Computer Science and Engineering, Shiv Nadar University, Chennai, India,
[1]sivapriyaofficial2005@gmail.com, [2] udayarajepadma@gmail.com

Abstract- **When blockchain and artificial intelligence converge, they hold the power to revolutionize the world much like the internet did in the past. Blockchain is a decentralized database that guarantees immutability and transaction permanence. On the other hand, artificial intelligence enables machines to perform activities that would otherwise need human intellect, such as data classification, pattern recognition, and prediction. Combining these two technologies will likely lead to exponential growth in several different industries. In this paper, we will review multiple models that integrate artificial intelligence and blockchain technology. Every model will be assessed during the review process according to the issues raised, the answers provided, the resources used, the benefits and drawbacks, and the results. These models present distinct perspectives on the reciprocal benefits of these technologies. The paper is centered on uncovering the potential of ongoing advancements in the fusion of blockchain and AI**.

Keywords: *Blockchain, Artificial Intelligence, Smart contracts, Distributed ledger, Decentralised Database, Ethereum.*

1. INTRODUCTION

The new internet is expected to be more stable due to its decentralized architecture, which eliminates the potential for a single point of failure. Customers won't need to worry about cancelling a particular account or dealing with service disruptions caused by malfunctions or other problems. By combining AI and blockchain, AI will be able to analyse data for complex decision-making. It can improve smart contract optimization by identifying flaws or inefficiencies in the logic or execution of the contract.

Blockchain technology offers a secure architecture that ensures information is stored with authorization, confidentiality, and integrity. As a result, a huge quantity of real data will be available for AI algorithms to train with

Blockchain:

Blockchain is a cryptographically secure distributed ledger that has the advantages of decentralisation, immutability, and transparency.

The database stores data in blocks that are linked together in a chain. It is like a giant interactive spreadsheet that everyone has access to. One major problem that has been fixed by the introduction of digital is double spending. (an individual utilising their digital currency more than once) To make sure the funds were only used once, a third-party system for transaction tracking was needed. Blockchain helps to mitigate this problem by using BitTorrent (a peer-to-peer encryption-based file sharing system).

Smart contracts:

Smart contracts in Ethereum are self-executing computer algorithms that enable mutually agreed terms and conditions for transactions, service exchanges, etc. The smart contract is unchangeable after it has been executed. After the code has been written and built in the Ethereum virtual machine, it is reviewed by each participating node in the transaction.

Consensus mechanism:

In the blockchain, a consensus mechanism is a system that verifies a transaction and marks it as authentic.

Proof of Work: PoW is a technique for validating blocks of transactions. This mechanism uses a game with a competitive reward system. They must employ complex algorithms to produce a hash value. The hash value generated should be less than the predetermined value. All the other nodes will verify the hash after it has been created and the block will then be put into the blockchain ledger.

Proof of stake: Compared to PoW, PoS requires less computational *power*. PoS uses a completely random validation mechanism instead of an inter-miner competition. A certain number of coins must be invested by a coin owner to become a validator. A block is considered approved for the chain when certain validators confirm for its validity. .

Proof of activity: PoA is a combination of both PoW and PoS. It takes the best features of both the consensus.

Artificial intelligence:

Artificial intelligence has made it possible for machines to perform tasks that people would typically be unable to complete by learning from experience and adapting to new inputs. The Checkers-playing Samuel was one of the first self- learning systems to be successful in the world and provided an early illustration of the fundamentals of artificial intelligence. Machine learning (ML) is a subset of AI that uses algorithms to learn patterns from data. Similarly, Deep learning (DL) is a subset of ML that employs artificial neural networks for complex tasks.

Machine learning	**Deep learning**
Supervised Learning	Deep neural networks
Unsupervised Learning	Artificial neural network
Reinforcement	Convolutional neural network

2. REVIEW

Securing data for AI with blockchain:

In [1] To accurately predict outputs, an AI model requires a training set with precise and unbiased data. However, internet information is often fragmented and controlled by a centralized authority. SecNet addresses this issue by constructing a secure blockchain framework for sharing tamper-proof data with guaranteed ownership. This model utilizes a Private Datacenter (PDC) to ensure uniform data access control. PDC incorporates Uniform Data Representation and Uniform Access Control (UDAC) to facilitate easy data exchange and provide control for authorized users. One key advantage of this model is its protection against Distributed Denial of Service (DDoS) attacks.

In [2] AIGC purchases in the metaverse are vulnerable to issues such as plagiarism, non-repudiation, and data leakage. The current Digital Access Management (DAM) systems use a trusted intermediary to manage AIGCs. MetaTrader proposes a blockchain-based DAM framework using smart contracts and an IPFS system to decentralize the purchase process between an AIGC seller and a customer. The encryption tools used to develop this model include AES-256 encryption (to produce a randomized symmetric key), SHA 256 Algorithm (to produce a hash for the encrypted data), and Elliptical curve encryption (to encrypt the symmetric key).

The key advantages of this model are protection against plagiarism after purchase, valid ratings for the AIGC product, prevention of denial of service, data leakage, unauthorized alterations, single point of failure, and non-repudiation. However, when this model is used in a consortium-chain, there is a high requirement for computation and storage, and the transaction per second is low. Additionally, due to tokens owned by different metaverse platforms, this model's incentive-based mechanism cannot easily adapt to their regulations.

In [3] Machine learning models require efficient and up-to-date datasets to stay current and generate reliable predictions. This framework allows users to collaboratively build a dataset without relying on a central authority to maintain the machine learning algorithm. To incentivize users to contribute high-quality data, this model incorporates specific incentive mechanisms using smart contracts and cryptographic hashes. Users can provide and update datasets within the blockchain, which may lead to inaccuracies and biases. Additionally, the model is challenging to use and not very user-friendly.

Using AI to secure blockchain:

In [4] Blockchain uses consensus methods like PoW and PoS to select miners. However, PoW uses an extensive amount of computational power to calculate the hash value required for validating the block. PoS, on the other hand, has the potential to centralize miner selection. Therefore, a new consensus mechanism called PoAI (proof of Artificial Intelligence) has been introduced. As miners play an integral part in the blockchain framework for validating transactions, PoAI is created with the help of a deep neural network (DNN) algorithm that predicts a suitable miner. The training dataset consists of the performance and actions of miners. The DNN algorithm uses stochastic gradient descent to minimize the loss function during training.

In [5] To identify vulnerabilities in a smart contract, the VulDet system uses a graph attention network (GAT). The GAT neural network is designed to analyze graph-structured data. VulDet focuses on two main types of vulnerabilities: re-entrancy (when external code is executed within the contract) and time dependency (exploiting the timestamp of a smart contract). Compared to other deep learning models for vulnerability detection, VulDet has demonstrated higher accuracy and efficiency in its results.

In [6] This paper proposes ENIGMA and its benefits over traditional smart contracts. ENIGMA are AI integrated smart contracts which provide ample benefits. They can form new predictions from past data and perform repetitive tasks in a much more efficient way without any human intervention.

The smart contract can be automatically deployed when the AI detects that certain parameters in the code are met. Mathematical models of enigma contracts include decision trees, neural networks, Bayesian networks. These deep learning algorithms enable the AI in smart contracts to be effectively trained using the given dataset. The main advantage of ENIGMA is that it detects frauds and cyber vulnerabilities in a smart contract without breaking the chain of blocks (consisting of transactions). While Artificial intelligence can identify patterns suggestive of common security weaknesses, they might struggle to identify more subtle or complex issues that require a greater comprehension of the underlying blockchain platform, and protocols.

In [7] Similar to ENIGMA, PPSC-BCAI also integrates Artificial intelligence with smart contracts to simplify system operations, service alerts, security threats, and false claims. For the experimental analysis, decision-tree, naïve Bayes, closest neighbour, and XGBoost are the algorithms utilised. Extreme gradient boosting, or XGBoost, is a machine learning method that learns from the dataset and produces more precise results. This model provides secure transactions and privatised smart contract access.

In [8] High computational and energy capacities may be needed for a proof of work process to validate a block of transactions. This paper proposes a framework called Curvetime which uses a machine learning algorithm called reinforcement learning. Each block represents the state of a Markov state machine. The act of making new blocks and connecting them together is a Markov decision process. A Markov decision process (MDP) is a stochastic decision-making process that uses a mathematical framework to simulate the decision-making of a dynamic system. (successive states depend on the current state). Tampering of data and cyber vulnerabilities are not possible due to the requirement of extensive computational power.

Integration of Blockchain and AI in different sectors:

Detection of Copyright infringement:

In [9] The use or creation of copyright protected content without the owner's consent is known as copyright infringement. This paper describes how blockchain technology, convolutional neural networks, and artificial neural networks can be used to identify this issue. A deep learning model called an ANN is used to detect patterns, criminal activity, dangerous JavaScript code, and speech. Another branch of AI that is only used for image analysis is CNN. Blockchain mostly establishes a framework for the preservation of rights and restricting access to data to authorised users in addition to these two algorithms.

Healthcare:

In [10] By facilitating safe and immutable preservation of patient information, blockchain lowers the frequency of health data breaches. This is due to the usage of asymmetric cryptography and hash functions. Medical records are used to train models like random forests, decision trees, Naive Bayes models, logistic and linear regression, support vector machines, and K-means clustering (unsupervised models) to perform specific analyses on complex data after blockchain provides tamper-free data for machine learning algorithms.

Integration of AI and blockchain with Real life applications

In [11] Due to the rising population, there is an intense demand for agricultural crops. However, by growing massive quantities of crops, the quality might rapidly decrease due to extensive use of pesticides. An AI-BC based model that can forecast excessive pesticide use in a crop is proposed in this research. Decision trees, support vector machines (SVM), perceptron, and random forest classifiers are among the models that are trained using input features derived from environmental and agricultural factors. A distributed and immutable blockchain ledger is integrated into the framework to store the predicted data from the machine learning algorithms. This, in turn, keeps unauthorised users from tampering with predicted results.

In [12] This paper presents a model that predicts whether a traffic event is true or false by combining a machine learning algorithm with a vehicular network. Vehicular networks are a subset of mobile computer networks in which individual automobiles interact with one another to serve as network nodes. The deep learning algorithms used are Convolutional Neural network and Bayesian inference. For a node (reporting vehicle), The credibility of a certain event is calculated with the help of 9 input features sent to the CNN algorithm. This credibility, ID, and message (broadcasted due to the event) are sent to the RSUs which provide a trust value of the node (Roadside Unit: A wireless device that provides connectivity and information between the passing vehicles). A dataset consisting of credibility and trust value is now sent to the Bayesian inference to provide the probability of the event (True or False). A double blockchain system is then used to form a strong connectivity between the blocks (consist of the trust value in its header, and credibility value in the body). This helps in preventing RSU attacks.

In [13] A smart transport public system uses a vehicular network by considering cars as nodes in a software application. This study presents a blockchain-based public transportation system's AI-enabled Distributed denial of service attack detection mechanism that can withstand a variety of cybersecurity threats. As each node in the chain is

encrypted with a hash value, even if one block is changed, the entire chain will be disrupted, which is why blockchain is employed to safeguard this system against integrity attacks. A Hybrid deep learning model is proposed by combining a 5 layered autoencoder (AE) and 3 layered multi-layer perceptron (MLP). While MLP is employed as a classifier to identify the sort of DDoS assault, AE is utilised as an unsupervised model to extract the attack's attributes. The algorithm's predictions were evaluated with the use of performance measurements like F1 score; of the three datasets, one had the lowest prediction accuracy at 84% of F1 score.

In [14] The integration of blockchain technology into the vaccine supply chain will improve vaccine security and enable greater accessibility for vaccine recipients. Decreased labour and low maintenance expenses for medical records boost the efficiency of management while minimising supply chain transaction costs. Artificial intelligence (AI) technology is expected to enhance the adaptability of the vaccine supply chain and build a flexible system that can synchronise vaccine production schedules and demand forecasts to avoid shortages and redundancies. The primary limitations of VSC are the costs of implementation, energy consumption, and complexity of the operations.

AI and blockchain with other domains:

Cyber Security:

In [15] Data protection is necessary in the modern era because of the rise in information sharing between various software applications. Blockchain technology and AI together therefore provide a multitude of solutions to this problem. AI models are trained with secure and untampered data stored in blockchain. These algorithms then offer a perceptive analysis of the reliability and vulnerabilities of the shared data. Moreover, AI plays a critical role in safeguarding users' security and privacy on the blockchain since all data is publicly accessible.

Internet of things:

In [16] Integrating IoT, AI and Blockchain could form a disruptive technology. They can be used in various applications such as healthcare, smart homes, supply chain and energy management. IoT connects multiple devices to one another and enables automated task execution using smart contracts. A blockchain provides a secure and distributed basis for data storage since the Internet of Things requires an abundance of data, and artificial intelligence facilitates data analysis, and intelligent decision-making. **[17]** The Industrial Internet of Things (IoT) will benefit from fast machine communication in addition to the influence of the 5G network.

3. CONCLUSION

The integration of Blockchain and AI presents a promising future in technology, offering unique capabilities that can revolutionize various industries. Through this research review, it becomes evident that the combination of Blockchain's secure, decentralized ledger and AI's advanced decision-making abilities holds immense potential for enhancing data security, transparency, and efficiency. Future research and models efforts should focus on addressing challenges such as scalability and user-friendliness while taking advantage of the strengths of both technologies to create more robust, inclusive, and ethical solutions. In conclusion, the integration of Blockchain and AI represents a transformative force with the potential to reshape industries, drive innovation, and empower individuals and organizations.

REFERENCES

[1] K. Wang, J. Dong, Y. Wang and H. Yin, (2019) "Securing Data With Blockchain and AI," in IEEE Access, vol. 7, pp. 77981-77989.

[2] V. T. Truong, H. D. Le and L. B. Le, "Trust-Free Blockchain Framework for AI-Generated Content Trading and Management in Metaverse," in IEEE Access, vol. 12, pp. 41815-41828, 2024, doi: 10.1109/ACCESS.2024.3376509.

[3] J. D. Harris and B. Waggoner, "Decentralized and Collaborative AI on Blockchain," (2019) IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 368-375, doi: 10.1109/Blockchain.2019.00057.

[4] Manjula K. Pawar, Prakashgoud Patil, Miner Selection in Blockchain using Proof of Artificial Intelligence, Procedia Computer Science, Volume 230, 2023, Pages 838-845.

[5] F. Luo and R. Luo, (2023) "VulDet: Smart Contract Vulnerability Detection Based on Graph Attention Networks," 2023 2nd International Conference on Artificial Intelligence and Blockchain Technology (AIBT), Zibo, China.

[6] M. Sultana, S. Thomas and N. Jayapandian, (2023) "Artificial Intelligence And Machine Learning Combined Security Enhancement Using ENIGMA," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakka.

[7] B D Deebak, Fadi AL-Turjman, (2021) Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements, Journal of Information Security and Applications, Volume 58, 2021,102749, ISSN 2214-2126.

[8] Jie You, Curvetime: A blockchain framework for Artificial Intelligence computation, software Impacts,Volume 13, 2022, 100314, ISSN 2665- 9638.

[9] A.Khare, U. Kumar Singh, S. Kathuria, S. V. Akram, M. Gupta and N. Rathor, "Artificial Intelligence and Blockchain for Copyright Infringement Detection," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, 2023, pp. 492- 496, doi: 10.1109/ICECAA58104.2023.10212277.

[10] 4M. Hassan, J. Chen, C. Zhu and U. Zukaib, , (2022) "Adoption of Blockchain-based Artificial Intelligence in Healthcare," 2022 5th International Conference on Artificial Intelligence and Big Data (ICAIBD), Chengdu, China, pp. 140-144, doi: 10.1109/ICAIBD55127.2022.9820137.

[11] Nilesh Kumar Jadav, Tejal Rathod, Rajesh Gupta, Sudeep Tanwar, Neeraj Kumar, Ahmed Alkhayyat, (2023) Blockchain and artificial intelligence-empowered smart agriculture framework for maximizing human life expectancy, Computers and Electrical Engineering, Volume 105, 108486, ISSN 0045-7906,

[12] X. Hu, (2023) "Artificial intelligence based trust management for vehicular networks using blockchain," 2023 8th International Conference on Information Systems Engineering (ICISE), Dalian, China, 2023, pp. 543-548,

[13] Liu, T., Sabrina, F., Jang-Jaccard, J., Xu, W., & Wei, Y. (2021). Artificial Intelligence-Enabled DDoS Detection for Blockchain-Based Smart Transport Systems. Sensors

[14] Ye Gao, Hongwei Gao, Han Xiao, Fanjun Yao, (2023) Vaccine supply chain coordination using blockchain and artificial intelligence technologies.

[15] R. Salama et al., (2023) "Blockchain Technology and Artificial Intelligence's Future Applications in Cyber Security," 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE), GHAZIABAD, India.

[16] Hu, H., Xu, J., Liu, M., & Lim, M. K. (2023). Vaccine supply chain management: An intelligent system utilizing blockchain, IoT and machine learning. Journal of business research.

[17] P. Pant et al., "Blockchain for AI-Enabled Industrial IoT with 5G Network," 2022 14th ECAI 2022,