Blockchain Frontier Technology (B-Front)
Vol. 4, No. 1, 2024, pp. 29∼34
E-ISSN: 2808-0009 P-ISSN: 2808-0831, DOI:10.34306

The Effectiveness of Using Blockchain Technology as A Machine Learning Program

Asep Sutarman[1*], Evelin Kallas[2], Oscar Jayanagara[3]
[1]Universitas Muhammadiyah Prof. Dr. HAMKA, Jakarta, Indonesia [2]Fakultas Sistem Informasi, Mfinitee Incorporation, Estonia [3]Universitas Pelita Harapan, Indonesia
[1]asepsutarmanmahcpud@gmail.com, [2]evellin@mfinitee.co.za, [3]oscar.fe@uph.edu
***Corresponding Author**

Article Info

Article history:

Received month dd, 2024-06-10
Revised month dd, 2024-07-05
Accepted month dd, 2024-07-30

Keywords:

Blockchain Technology
Machine Learning
Effectiveness

ABSTRACT

Several successful papers and applications have demonstrated machine learning's limitless potential. However, when we immerse ourselves in powerful machine learning-based systems or applications, two critical research issues arise: how to ensure that the searched results of a machine learning system are not tampered with by anyone and how to prevent other users in the same network environment from easily obtaining our private data. This predicament is similar to that of other modern information systems that face security and privacy concerns. The introduction of blockchain technology presents us with an alternate method of addressing these two challenges. As a result, recent research has sought to construct machine learning systems using blockchain technology or to apply machine learning methods to blockchain systems. In this study, we provided a parallel framework to identify acceptable deep learning hyperparameters in a blockchain context using a metaheuristic algorithm to demonstrate what the combination of blockchain and machine learning is capable of. The suggested system also takes communication costs into consideration by restricting the amount of information transfers between miners and blockchain.

1. INTRODUCTION

For years, the development of artificial intelligence (AI)[1]. has experienced significant changes, with various successful applications being given to the public to provide us with a more convenient existence today. One of the most significant research streams of AI technologies is undoubtedly machine learning (ML) with three typical learning technologies termed supervised, unsupervised, and semi-supervised, correspondingly][2]. Each of these three technologies can be employed alone in an intelligent system; however, they can also be combined if necessary to solve a problem [3]. The core notion of machine learning, as an important AI research path, is to use labeled/unlabeled input data to identify the proper rules to categorize yet unknown data or to anticipate events in the future. Both supervised and unsupervised learning have a learning method, as illustrated in Fig. 1. The fundamental distinction is that the first input data of supervised learning are labeled data, whereas the first input data of unsupervised learning are unlabeled data. As a result, they require quite distinct learning techniques. Because unsupervised learning requires less information than supervised learning to categorize unlabeled data, it is more efficient. In contrast, supervised learning will utilize the labeled data to build the

model that will categorize the unlabeled data. As a result, supervised learning often outperforms unsupervised learning in terms of accuracy. Of course, this does not mean that unsupervised is no longer effective; on the contrary, it is quite valuable when obtaining labeled data for the machine learning system is difficult[4].

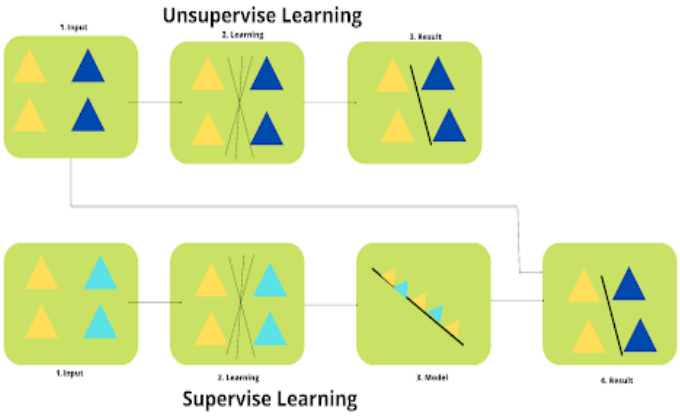

Figure 1. Supervise Unsupervised Learning

Aside from determining possible applications for AI and ML technologies, two major research concerns today are how to safeguard intelligent systems from being attacked by abnormal users and how to secure the privacy of private and sensitive data in intelligent systems [5]. Because machine learning and blockchain technology emerged from two distinct fields, their design and goals are extremely distinct. One significant distinction is that most machine learning technologies are built for an integrated perspective, combining data and calculations from one or more computers, whereas most blockchain technologies are designed for a peer-to-peer view, dividing data and computations over several computers. This is the primary reason why parallel computing has emerged as one of the most current developments in research on integrating machine learning and blockchain technology into a single information system [6].

That is why this article focuses on machine learning-based blockchain frameworks, because a good ML framework would aid us in developing an effective method of combining ML with blockchain technologies or applying ML to blockchain systems [7].

As a result, the key contributions of this work might be stated as follows:

1. It begins with a quick overview of the parallel ML frame-works with blockchain technologies and their application. to blockchain systems, serving as a road plan for integrating ML and blockchain.

2. It then provides a full description of the proposed parallel deep learning framework with blockchain as the focal point. emphasis focused on discovering ”excellent” deep learning hyperparameters by employing a metaheuristic method to further increase accuracy that relies on the collaboration of all nodes.

effective approaches to speed up machine learning algorithms have been proposed dating back to the 1980s or even earlier, because parallel computing is an easy and helpful way to minimize the reaction time of machine learning algorithms [8]. How to apply machine learning techniques to parallel computing settings has been a major research area since the 1990s. Although the concepts of distributed computing and parallel computing in early research were considerably distinct, the line between them has grown hazy in subsequent studies [9].

The main reason is that in distributed computing, each processor (node) has its own memory, whereas all processors (nodes) will access a shared memory, but some recent studies in the machine learning research domain used the name parallel machine learning algorithm to describe the algorithms they proposed, for which each node has its own memory [10]. It should be noted that in this study, the term ”parallel” refers to both parallel and distributed computing [11]. These three parallel models are also seen in several metaheuristic techniques, such as particle swarm optimization (PSO) [12]. ivided parallel PSOs into three groups and discussed them PSO’s capabilities in different distributed computing environments, such as CPU vs. GPU or PSO topology [13].

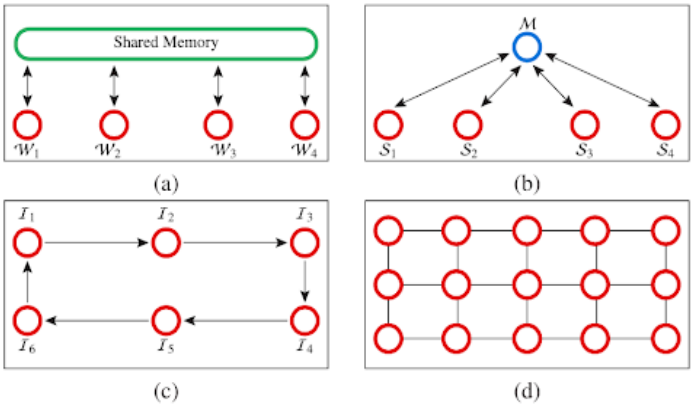

Figure 2. Parallel Machine Learning

As illustrated in Fig. 2, we add a new category to these three: multithreading (or shared memory) to cover parallelism on the same machine but employing several threads for parallel processing. As shown in Fig. 2(a), all of the threads Wi share the same information via shared memory. Fig. 2(b) indicates that, while master-slave slave nodes Si will exchange the same information via master node M, the primary distinctions are that slave nodes are controlled by master node and all slave nodes are different. Figures 2(c) and (d) illustrate that each coarse-grained node transfers its searched information to another node, whereas each fine-grained node distributes its sought information to a collection of neighbor nodes [14], [**?**].

To summarize, there are several approaches to classify simultaneous machine learning and deep learning algorithms [15]. for example, categorized parallel machine learning techniques based on topological structures into four categories: (1) ensembling, (2) tree, (3) parameter server, and (4) peer-to-peer [16].

significant characteristics to characterize distributed deep learning algorithms are model consistency, parameter distribution and communication, and training distribution [17]. Our investigation covers topics including supply chain trust, blockchain execution environment, and smart contract design [18]. The goal of this comprehensive approach is to offer a strong foundation for comprehending and addressing the security risks associated with BC-SCM systems[19].

This paper attempts to provide a thorough knowledge of the obstacles preventing the construction of security and dependability in BC-SCM systems by utilizing insights from academics and industry[20]. In addition to identifying these issues, this paper suggests solutions, establishing the framework for additional study and the development of workable security in BC-SCM systems. We hope to improve the robustness and resilience of BC-SCM systems by tackling these important problems, so that they can fulfill their potential to revolutionize supply chain management[21].

2. RESEARCH METHOD

lockchain can provide a safe and private mechanism to transfer messages between information systems on the internet and will radically modify the architecture of portion of information transmission in particular information systems. Blockchain development may be traced back to the 2008 publication of the bitcoin white paper. Because it was born in that year, the majority of internet technologies and hardware have matured greatly. In comparison to the 1980s. Because the blockchain was created in a distributed computer environment, The distributed ”ledger” approach allows the ”transactions” to be kept in more than one node [1]. These attributes allow the blockchain to provide a more robust means of achieving the goals of permanent tracking, provenance history, and immutability. Of course, the architecture of blockchain takes security and privacy concerns for data (transactions) exchange and transmission in such a novel network environment into account [22].

Several recent studies have identified two potential research topics: (1) utilizing AI to improve the performance of a blockchain system and (2) using blockchain to improve the security and privacy of data and model transfer on an AI system. [23].

As illustrated in Fig. 3, Ferrag and Maglaras [26] proposed a blockchain-based energy scheme that allows smart grid network nodes to sell surplus energy to surrounding nodes (e.g., HAN) or neighbors on the

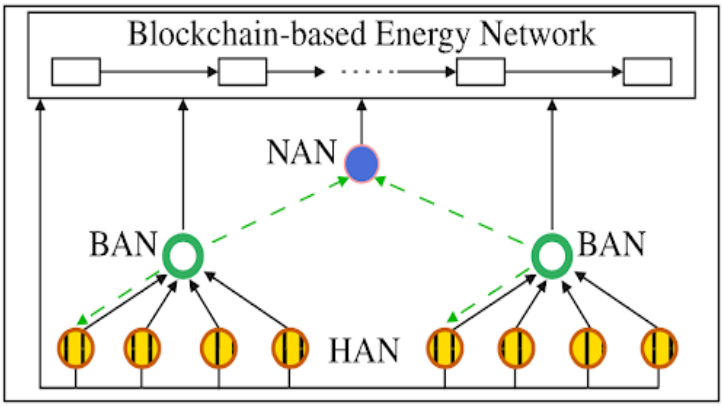

Figure 3. Blockchain based Energy Network

opposite side of the street (e.g., building area network (BAN) and neighborhood area network (NAN) (NAN). In Fig. 3, the dot line symbolizes energy currency for the consumer to sell/buy energy from adjacent nodes [24]. The home area network (HAN) is at the bottom of the hierarchy. Fig. 6; if necessary, it can deliver extra energy to neighboring neighborhoods. This method is comparable to the A shared memory parallel computing method for sharing data among HAN, BAN, and NAN nodes [25].

1. Using the Byzantine process, miner nodes must be validated by at least 51% of all nodes in the network before their data may be added to the blockchain. This incurs significant extra compute and communication expenses, degrading miner node performance while addressing an optimization problem.
2. When attempting to deploy blockchain and machine learning technologies to devices in an internet of things context, it is necessary to consider the processing limitations of such devices.
3. Because communication between miners and blockchain or between miners requires a significant amount of waiting, verification, and processing, a parallel machine learning framework for such an environment must minimize the frequency of communication between miners and blockchain or between miners.

To summarize, while parallel machine learning for blockchain is still in its early stages of development, there are many opportunities to build far better approaches to improve the performance of such a system [26].

3. RESULT AND DISCUSSION

The MNIST dataset (http://yann.lecun.com/exdb/m nist/) is used to train the DNN classification model to evaluate the performance of the proposed framework (PDLKC). Grid search (GS) and simulated annealing (SA) [27]. User to discover acceptable DNN hyperparameters, i.e. to solve the hyperparameter optimization issue [28].

Both GS and the proposed framework were written in Python, and the blockchain was Ethereum (web3 5.20.0 and solidity 0.5.0). In the simulation, three PCs running Ubuntu 18.04.5 LTS are utilized, and the miner node applications are developed in Python 3.6.9. These three PCs have varied CPUs, GPUs, RAM capacities, and even run different versions of TensorFlow, as seen in Table 1 [29].

Table 1. Environment for Miner Nodes

Miner	CPU	Memory	GPU	TensorFlow
M1	AMD Ryzen 5 3600X 6-Core Processor	32 GB	GeForce RTX 3080 and CUDA 11.1	2.4.0
M2	Intel Core i9-9900X CPU (3.60 GHz)	32 GB	GeForce RTX 2080 Ti and CUDA 11.2	2.3.0
M3	Intel Core i9-9820X CPU (3.30 GHz)	128 GB	GeForce RTX 2080 Ti and CUDA 11.2	2.4.1

Our observations indicate that this is related to the fact that the proposed framework's miner nodes do not regularly upload the findings to blockchain. This implies that when a miner node receives a solution s

(a collection of hyperparameters) from blockchain, it will construct a few solutions based on the solution s in order to train the DNN models. After obtaining a set of models, each miner node will upload one of the best solutions to the blockchain. This reduces communication costs between miner nodes and the blockchain, as well as waiting time imposed by other mining nodes.

This comparison clearly shows the benefits of using ML to a blockchain context to improve response time. The suggested framework may be utilized to solve an optimization issue by combining supervised and unsupervised learning approaches. The suggested architecture has two drawbacks as a result of Ethereum implementation constraints. The first is that all parameters (including hyperparameters) must be encoded as integer numbers, while the second is because the blockchain environment cannot manage too many processing activities (or transactions). In summary, the proposed framework's strength is that it provides a feasible solution to link ML with blockchain while also lowering ML training time. The shortcomings of the framework is that still some unnecessary waiting times incur among the miner nodes.

4. CONCLUSION

In this research, we presented a straightforward yet effective parallel deep learning architecture designed specifically for blockchain environments. The key feature of the proposed framework is its ability to leverage the blockchain's inherent characteristics, ensuring that the model on the knowledge chain is validated by a majority of miner nodes. This mechanism provides a secure method for obtaining the trained model, aligning with the decentralized nature of blockchain technology.

However, the suggested framework is not without its challenges. It faces some of the same difficulties encountered in other parallel machine learning systems within blockchain environments. Specifically, these issues include (1) higher communication costs related to the transfer of data, models, and parameters, and (2) unnecessary delays caused by synchronization and communication processes. These factors can impact the efficiency and scalability of the system.

To address these limitations, we aim to develop improved solutions in future work. By focusing on reducing communication overhead and minimizing synchronization delays, we hope to enhance the overall performance and efficiency of the proposed framework, ultimately making it more suitable for real-world applications in blockchain-based deep learning systems.

REFERENCES

[1] Y. Li and T. Chen, "Blockchain empowers supply chains: challenges, opportunities and prospects," *Nankai Business Review International*, vol. 14, no. 2, pp. 230–248, 2023.

[2] T. K. Vashishth, V. Sharma, K. K. Sharma, B. Kumar, S. Chaudhary, and R. Panwar, "Security and privacy challenges in blockchain-based supply chain management: A comprehensive analysis," in *Achieving Secure and Transparent Supply Chains With Blockchain Technology*. IGI Global, 2024, pp. 70–91.

[3] B. Pan, L. Zhang, C. Li, and L. Chen, "Supply chain management system's cybersecurity based on blockchain technology," *International Journal of Science and Advanced Technology*, vol. 11, 2023.

[4] A. Singh, S. H. Krishna, A. Tadamarla, S. Gupta, A. Mane, and M. Basha, "Design and implementation of blockchain based technology for supply chain quality management: Challenges and opportunities," in *2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM)*. IEEE, 2023, pp. 01–06.

[5] A. Karunamurthy, T. A. Victoire, S. Sunali, and P. Thamizharasi, "Block-chain management in supply chain management—a comprehensive review," *Supply Chain Management*, vol. 13, pp. 06–2023, 2023.

[6] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, and U. Biswas, "Blockchain for intelligent transportation systems: Applications, challenges, and opportunities," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18 961–18 970, 2023.

[7] N. Md Nasir, K. Mohd Zaini, S. Hassan, and N. Nordin, "Blockchain-based supply chain for a sustainable digital society: Security challenges and proposed approach," in *International Conference on Computing and Informatics*. Springer, 2023, pp. 44–57.

[8] X. Xu, L. Tatge, X. Xu, and Y. Liu, "Blockchain applications in the supply chain management in german automotive industry," *Production Planning & Control*, vol. 35, no. 9, pp. 917–931, 2024.

[9] O. I. Oriekhoe, B. I. Ashiwaju, K. C. Ihemereze, U. Ikwue, and C. A. Udeh, "Blockchain technology in supply chain management: a comprehensive review," *International Journal of Management & Entrepreneurship Research*, vol. 6, no. 1, pp. 150–166, 2024.

[10] J. Aslam, A. Saleem, and Y. B. Kim, "Blockchain-enabled supply chain management: integrated impact on firm performance and robustness capabilities," *Business Process Management Journal*, vol. 29, no. 6, pp. 1680–1705, 2023.

[11] S. Turgay, S. Erdoğan *et al.*, "Enhancing trust in supply chain management with a blockchain approach," *Journal of Artificial Intelligence Practice*, vol. 6, no. 6, pp. 56–64, 2023.

[12] F. Sunmola and P. Burgess, "Transparency by design for blockchain-based supply chains," *Procedia Computer Science*, vol. 217, pp. 1256–1265, 2023.

[13] O. Shmatko, J. Litvinova, and M. Shokin, "New blockchain-based supply chain management system model," *Scientific Collection InterConf+*, no. 33 (155), pp. 470–479, 2023.

[14] J. Liu, H. Zhang, and L. Zhen, "Blockchain technology in maritime supply chains: applications, architecture and challenges," *International Journal of Production Research*, vol. 61, no. 11, pp. 3547–3563, 2023.

[15] M. Uddin, S. Selvarajan, M. Obaidat, S. U. Arfeen, A. O. Khadidos, A. O. Khadidos, and M. Abdelhaq, "From hype to reality: Unveiling the promises, challenges and opportunities of blockchain in supply chain systems," *Sustainability*, vol. 15, no. 16, p. 12193, 2023.

[16] M. R. Khan, M. R. Khan, and K. Nallaluthan, "Blockchain supply chain management and supply chain sustainability," in *Blockchain Driven Supply Chain Management: A Multi-dimensional Perspective*. Springer, 2023, pp. 155–180.

[17] A. Yazdinejad, E. Rabieinejad, T. Hasani, and G. Srivastava, "A bert-based recommender system for secure blockchain-based cyber physical drug supply chain management," *Cluster Computing*, vol. 26, no. 6, pp. 3389–3403, 2023.

[18] M. A. Alqarni, M. S. Alkatheiri, S. H. Chauhdary, and S. Saleem, "Use of blockchain-based smart contracts in logistics and supply chains," *Electronics*, vol. 12, no. 6, p. 1340, 2023.

[19] E. Yontar, "The role of blockchain technology in the sustainability of supply chain management: Grey based dematel implementation," *Cleaner Logistics and Supply Chain*, vol. 8, p. 100113, 2023.

[20] H. Malik, T. Anees, M. Faheem, M. U. Chaudhry, A. Ali, and M. N. Asghar, "Blockchain and internet of things in smart cities and drug supply management: Open issues, opportunities, and future directions," *Internet of things*, p. 100860, 2023.

[21] J. Liu, G. Yeoh, L. Gao, S. Gao, and O. Ngwenyama, "Designing a secure blockchain-based supply chain management framework," *Journal of Computer Information Systems*, vol. 63, no. 3, pp. 592–607, 2023.

[22] L. Zhou, A. Diro, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *Journal of Information Security and Applications*, vol. 80, p. 103678, 2024.

[23] W. Shafik, "Blockchain-based internet of things (b-iot): Challenges, solutions, opportunities, open research questions, and future trends," *Blockchain-based internet of things*, pp. 35–58, 2024.

[24] S. Datta and S. Namasudra, "Blockchain-based secure and scalable supply chain management system to prevent drug counterfeiting," *Cluster Computing*, pp. 1–18, 2024.

[25] L. Hong and D. N. Hales, "How blockchain manages supply chain risks: evidence from indian manufacturing companies," *The International Journal of Logistics Management*, 2023.

[26] S. Kolasani, "Blockchain-driven supply chain innovations and advancement in manufacturing and retail industries," *Transactions on Latest Trends in IoT*, vol. 6, no. 6, pp. 1–26, 2023.

[27] X. Zhang, X. Feng, Z. Jiang, Q. Gong, and Y. Wang, "A blockchain-enabled framework for reverse supply chain management of power batteries," *Journal of Cleaner Production*, vol. 415, p. 137823, 2023.

[28] E. K. Kambilo, I. Rychkova, N. Herbaut, and C. Souveyet, "Addressing trust issues in supply-chain management systems through blockchain software patterns," in *International Conference on Research Challenges in Information Science*. Springer, 2023, pp. 275–290.

[29] R. Alajlan, N. Alhumam, and M. Frikha, "Cybersecurity for blockchain-based iot systems: a review," *Applied Sciences*, vol. 13, no. 13, p. 7432, 2023.