VIVA-Tech International Journal for Research and Innovation *Volume 1, Issue 6 (2023)* ISSN(Online): 2581-7280

VIVA Institute of Technology

11th National Conference on Role of Engineers in Nation Building – 2023 (NCRENB-2023)

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION

ANNUAL RESEARCH JOURNAL

ISSN(ONLINE): 2581-7280

Blockchain & Machine Learning In Communication

Prof.Sonia Dubey[1], Pratiksha Pawar[2], Yashashree Kulkarn[3]

[1](MCA, Viva Institute of Technology/Mumbai University, India)

[2](MCA, Viva Institute of Technology/Mumbai University, India)

[3](MCA, Viva Institute of Technology/Mumbai University, India)

Abstract: *Blockchain can greatly facilitate the sharing of training data and ML models, decentralized intelligence, security, privacy, and reliable ML decision making. On the other hand, ML will have a significant impact on the development of blockchain in communication and network systems, including energy and resource ef iciency, scalability, security, privacy, and smart contracts. However, there are some outstanding key issues and challenges that still need to be addressed before blockchain and ML integration becomes mainstream, including resource management, data processing, scalable operations, and security issues. In this article, we provide an overview of existing work for blockchain and ML technologies. We identify several key aspects of blockchain and ML integration, including an overview, benefits, and applications. Next, we discuss open questions, challenges, and broader perspectives that need to be addressed to consider blockchain and ML for communication and network systems together.*

.Keywords – *Blockchain, communication, Learning, Machine, technology.*

I. INTRODUCTION

Integration of blockchain and ML, including overview, benefits and applications. We then discuss some outstanding issues, challenges and broader perspectives that need to be addressed in order to jointly consider blockchain and ML for communication and networking systems. Blockchain and ML integration, including overview, benefits and applications. We then discuss some outstanding issues, challenges, and broader perspectives that need to be addressed to jointly consider blockchain and ML for networking and communication systems. Blockchain and ML integration, including overview, benefits, and applications. We then discuss some outstanding issues, challenges, and broader perspectives that need to be addressed to jointly consider blockchain and ML for networking and communication systems. Blockchain, the technology behind digital cryptocurrency, has attracted a lot of attention from both academia and industry.[1]

Blockchain is essentially a distributed ledger operated by network participants in a logical peer-to-peer (P2P) network. It creates a paradigm of trust Integration of blockchain and ML, including overview, benefits and applications. We then discuss some outstanding issues, challenges and broader perspectives that need to be addressed in order to jointly consider blockchain and ML for communication and networking systems. Blockchain and ML integration, including overview, benefits and applications. We then discuss some outstanding issues, challenges, and broader perspectives that need to be addressed to jointly consider blockchain and ML for networking and communication systems. Blockchain and ML integration, including overview, benefits, and applications. We then discuss some outstanding issues, challenges, and broader perspectives that need to be

addressed to jointly consider blockchain and ML for networking and communication systems. Blockchain, the technology behind digital cryptocurrency, has attracted a lot of attention from both academia and industry.

between humans and machines and allows applications to operate without central control or intermediaries. In general, blockchain is included in a number of distributed ledger technologies, which employ a variety of mechanisms for recording and sharing transactions and data across multiple nodes in a decentralized manner.

However, distributed ledger structures are not just a chain of blocks, but other structures as well. Blockchain has opened up a number of promising opportunities for a variety of applications and scenarios by efficiently developing P2P platforms for information sharing, improving governance enforcement, and increasing resource utilization. According to McKinsey, blockchain technology could reach its full potential within the next five years in any application using a centralized solution, based on the current rate of evolution.[2].

Blockchain-based solutions, in particular, have changed communication and network systems thanks to their key characteristics compared to traditional solutions. They provide a valid solution for dynamic access control, the integrity and validity of the data exchanged and the privacy of mobile users. Such a decentralized and distributed blockchain can, for example, be applied in ad hoc networks, where intelligent end devices connect without central base stations. For simplicity, we use the term "blockchain technology" here to refer to general classes of distributed ledgers based on community consensus.[3]

They provide a viable solution for dynamic access control, integrity and validity of exchanged data, and mobile user privacy. Such a decentralized and distributed blockchain can be used, for example, in ad hoc networks in which intelligent terminals connect without central base stations. They can also be applied in fog or cloud radio access networks to maintain tight synchronization between different network elements equipped with computing and networking resources. The researchers provided the systematic overviews of the blockchain and demonstrated the broad application possibilities of the blockchain.[4]

II. BLOCKCHAIN USE FOR COMMUNICATION

Email is the most common network application and authentication between users is an important feature. The most commonly used approaches to ensure this property are PKI and S/MIME email encryption protocols, but in fact they are exposed to multiple security threats such as: B. MITM attack and EFAIL attack . Blockchain is an innovative technology that overcomes these threats and decentralizes sensitive operations while maintaining a high level of security. Eliminate the need for trusted intermediaries. The blockchain is accessible to all nodes in the network and keeps track of all transactions already made. The aim of our work is to offer a secure messaging solution based on blockchain technology.[5]

In this article, we explain why blockchain would make communication more secure, and we propose a model design for blockchain-based messaging that improves the performance and security of data recorded on the blockchain by using a smart contract to verify the identities and the associated public key maintained. and validate the user certificate. The system is fully decentralized and allows users to exchange messages securely.[6]

2.1 Why Blockchain would Makes Communication More Secure

Blockchain-based messaging that maintains the performance and security of data stored on the blockchain by using a smart contract to verify identities and their associated public keys and to validate the user's certificate. The system is fully decentralized and allows users to exchange messages securely. The blockchain is decentralized and no centralized authority can approve transactions. All network participants must reach a consensus to securely validate transactions, and previous records cannot be changed. Blockchain-based messages that maintain the performance and security of data recorded on the blockchain, using a smart contract to verify identities and associated public keys and validate the user certificate. The system is fully decentralized and allows users to exchange messages securely.[5]

Due to the decentralised nature of the blockchain, no centralised authority can approve transactions. To safely validate transactions, all network users must come to an agreement, and historical data cannot be modified. transactions, a timestamp, a reference to the block before it, and is encrypted. It is safe because:

1. Public Key Infrastructure: It uses public/private key encryption and data hashing to securely store and share data.
2. ledgers: there is no central authority to hold and store data, removes single point of failure

3. Peer-to-peer network: The communication is based on the P2P network architecture and inherits the decentralized
4. cryptographic techniques, hash functions, Merkle trees, public and private keys. Difficult to change blockchain, to make a change it is necessary to succeed in a simultaneous attack on more than 51% of the participants.
5. Consensus Algorithm: The rules followed by network nodes to verify the distributed ledger. Consensus algorithms are designed to achieve reliability in a system with multiple untrusted nodes. A consensus of the nodes validates the transactions.
6. The choice of consensus algorithm has a significant impact on performance, scalability, latency, and other blockchain parameters. Consensus algorithms must be fault tolerant.[6]

2.2 Machine Learning Use For Communication.

Machine learning is a term used in the field of computer science that evolved from the consideration of structure confirmation and computer learning theory of artificial intelligence. Communication systems produce a lot of traffic data; It is a comprehensive upgrade to network and communications planning and management when combined with an advanced machine learning process. Machine learning is an advanced part of computer algorithms designed to track human intelligence by learning from the big picture. It is considered the new era of huge amounts of data. Machine learning-based approaches have been successfully applied in various fields such as computer vision, communication technologies, engineering, finance, and entertainment, etc. Machine learning and communication technologies are combined in various fields.[7]

We focus on the use of machine learning for communication networks. Wireless communication networks are considered as a rudimentary paradigm evolving towards radio intensive and intelligent environments. The main question surrounding the task of deep learning in such communication networks is not whether it will be a fundamental part of future networks, but rather when and how to activate this mix. As the name suggests, it is a visual guiding communication and is depicted as carrying thoughts and information in structures that can be visualized or viewed. It depends solely and entirely on the vision, and in reality they are two-dimensional images given or communicated. It consists of: fonts, shadows, visual automation, delineation, typography, drawings and electronic resources. An insurance system contains two areas: the characterization tool or encryption process for the information and a subsystem of a key organization. This recommendation describes key organization and confirmation procedures for a security system suitable for use in a variety of bandwidth-constrained media organizations. Certainty is cultivated through the use of puzzle keys.[8]

2.3 Blockchain Benefit Machine Learning And Cammunication.

With key blockchain features including decentralization, immutability, and transparency, blockchain provides a new opportunity for ML algorithms used in communication and network systems to detect potential impacts and impacts of these technologies and take steps to mitigate negative impacts and reduce effects.

A. Blockchains can Benefit Machine Learning for Data and Model Sharing.

Network and communication systems applying ML solutions typically contain a large amount of data, such as training on large datasets or processing high-throughput streams. With more data to analyze, the machine's predictions and decisions are considered more accurate, and the trained models and algorithms are more reliable. Blockchains allow data sharing and storage without relying on third parties by exploring a number of existing technologies, including transaction timestamping, cryptography, P2P networks, etc. In particular, data and information can be time stamped in a decentralized and sabotage environment. test way. Cryptography ensures secure transmission of data and\nallows immutability of records in decentralized P2P networks. For example, the data is hashed and the hash can be incorporated into a transaction stored on the blockchain, providing definitive proof of the exact time the data existed. \nFurthermore, a blockchain is a read-only immutable data structure, where new blocks are added to the end of the ledger by linking to the hash identifier of the previous block. In this way, the blockchain supports the secure sharing and storage of data in trusted networks. The Ocean Protocol is a

decentralized platform that uses blockchain technology to share data and AI models in a secure and transparent way. The Ocean decentralized network has three main tiers:

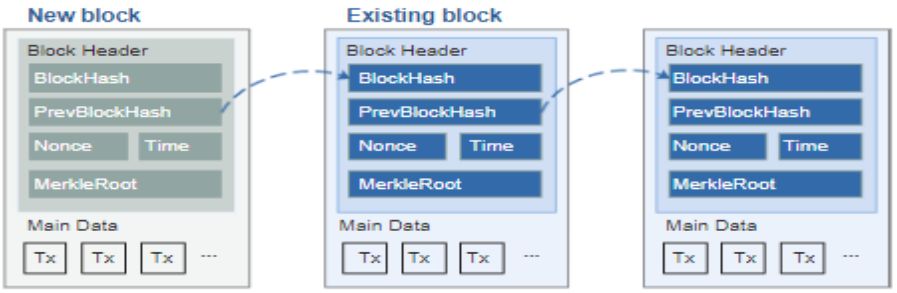
1) the Keeper tier which manages SLAs, low-level access control, accounts, balances, and the incentive (or block reward) scheme.

2) The level of authentication that cryptography introduces challenges to the integrity and security improvement of services.

3)the level of care serving as a discovery mechanism, as well as reporting and governance aspects. Table IV lists the roles that participate in the Ocean network.

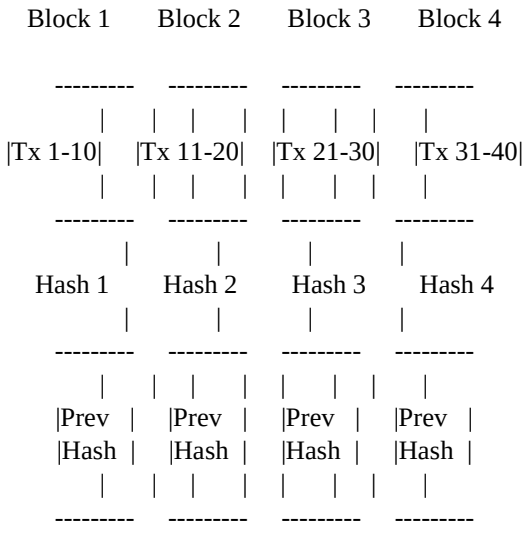
In the platform, data providers can upload their data and monetize it by publishing it, while data consumers can discover and buy data to build innovative applications. Custodians implement Service Level Agreements (SAs) as smart contracts that remove the middleman between data providers and consumers. An incentive mechanism is proposed to encourage participants/users to operate holders. In particular, the data consumer needs demonstrably correct model execution on the purchased data. To solve this problem, verification layer verifiers are responsible for verifying and enforcing services and conditions in SAs by issuing challenges to provers and verifying the returned proof[9]

2.4. Illustration Of a Chain Of Block



A chain of blocks, also known as a blockchain, is a digital ledger that records transactions in a secure and transparent manner. Each block in the chain contains a record of multiple transactions, along with a unique cryptographic hash that identifies the block and links it to the previous block in the chain.[10]

Here is an illustration of a chain of blocks:



In this illustration, we can see four blocks in the chain. Each block contains a set of transactions (Tx 1-10, Tx 11-20, Tx 21-30, and Tx 31-40) and a unique cryptographic hash (Hash 1, Hash 2, Hash 3, and Hash 4).[11]

The hash of each block is created using a mathematical function that takes the data in the block as input. This function produces a fixed-length string of characters that is unique to the block. The hash also includes the hash of the previous block in the chain, which links the blocks together in a linear sequence.

The last block in the chain (Block 4) includes a reference to the hash of the previous block (Hash This means that any change to the data in Block 3 would also change the hash of Block 4, making it impossible to tamper with the data without being detected.

This chain of blocks illustrates the fundamental concept of a blockchain and how it provides a secure and secure and transparent way to record and track transactions.[12]

III. METHODOLOGY

Blockchain and machine learning are two powerful technologies that can be used in communication methodologies to improve efficiency, security, and accuracy.Blockchain is a decentralized digital ledger that allows multiple parties to securely store and share information without the need for intermediaries. This technology can be used in communication methodologies to create transparent and immutable records of transactions and data exchanges, which can increase trust and reduce the risk of fraud.Machine learning, on the other hand, is a subset of artificial intelligence that involves training algorithms to learn from data and make predictions or decisions without being explicitly programmed. This technology can be used in communication methodologies to automate tasks, analyze large amounts of data, and personalize interactions with users.When combined, blockchain and machine learning can create powerful communication methodologies that are both secure and intelligent. For example, blockchain can be used to store and verify data, while machine learning can be used to analyze and extract insights from that data. This can lead to more targeted and effective communication strategies, as well as improved customer experiences.Overall, the integration of blockchain and machine learning in communication methodologies has the potential to revolutionize the way organizations communicate with their stakeholders, by providing them with more secure, efficient, and personalized interacti.[13]

IV. CONCLUSION

blockchain and ML, which is becoming a necessary solution that enables intelligent, secure and decentralized sharing of data and models, as well as efficient operation of network and communication systems. We first provided an overview of blockchain and ML, briefly introducing the basic concepts, taxonomies and typical ap-s. We then presented some key features of blockchain (decentralization, transparency, security, immutability, etc.) that can benefit ML documents, including data and model sharing, security and privacy, decentralized intelligence, and trusted decision-making. Furthermore, we have demonstrated that machine learning can benefit several aspects of the blockchain, including energy and resource efficiency, scalability, security and privacy, and smart contract implementation. Additionally, we discussed some outstanding issues for future research, such as big data processing, scalability, security and privacy, efficient consensus protocols, and resource management. Finally, we explored some broader perspectives such as IoT, big data and edge computing to identify further research opportunities.

In summary, research into integrated blockchain and machine learning for communication and networking is quite extensive and a number of challenges lie ahead. This paper briefly attempts to examine the technologies associated with integrating blockchain and ML at a very preliminary level and to discuss future research that could benefit from pursuing this vision. Our contribution benefits from a fully decentralized architecture that provides inherent fault tolerance, redundancy and transparency. We first proposed an approach that enables secure communication and benefits from the security properties of blockchain.

We plan to implement our proposal to empirically support our results and demonstrate its feasibility. Our next proposal is to implement a smart contract architecture to validate, store and revoke the certificate on a public blockchain. Theperson's certificate contains their address and public key, the address of the smart contract that issued it and stored it off-chain.

ACKNOWLEDGEMENT

This research would not have been possible without the help and support of many people, and we are very honored to have received it during the completion of the work. We would also like to thank our project manager Prof. Sonia Dubey for sharing pearls of wisdom with us throughout this research. We are also extremely grateful to our teachers, friends, and families who guided us with insightful comments that helped us complete our research work. Everyone's generosity and expertise enhanced this research paper in countless ways. We are grateful and fortunate enough to receive constant encouragement, support and guidance from all teaching staff who have helped us to successfully complete our work.

REFERENCES

[1] Lakshmi Siva Sankar,Sindhu M,M. Sethumadhavan: Survey of Consensus Protocols on BlockchainApplications, International Conference on Advanced Computing and Communication Systems (ICACCS -2017).
[2] Du Mingxia, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, Chen Qijin: A Review on the ConsensusAlgorithm of Blockchain, IEEE (2017).
[3] Guy.z, Oz.N, Alex.P: Decentralized Privacy: Using Blockchain to Protect Personal Data, (2018) .
[4] S. Nakamoto. (2008) Bitcoin: A peer-to-peer electronic cash system. [Online]. Available:
[5] F. M. Benˇci´c and I. P. ˇZarko, "Distributed ledger technology: Blockchain compared to directed acyclic graph," in Proc. IEEE ICDCS 18, July 2018, pp. 1569–1570.
[6] X. Jiang, F. R. Yu, T. Song, Z. Ma, Y. Song, and D. Zhu, "Blockchain-enabled cross-domain objectdetection for autonomous driving: Amodel sharing approach," IEEE Internet of Things Journal, 2020.
[7] R. Graf and R. King, "Neural network and blockchain based technique for cyber threat intelligence and situational awareness," in Proc. Cy-Con'18, May 2018, pp. 409–426.
[8] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A staofthe art survey," IEEE Comm.Survey and Tutorials, pp. 1–1, 2018.
[9] V. Buterin and V. Griffith, "Casper the friendly finality gadget," arXiv preprint arXiv:1710.09437, 2017.
[10] C. Cachin, "Architecture of the hyperledger blockchain fabric," in Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol. 310, 2016.
[] M. Salimitari and M. Chatterjee, "An overview of blockchain and con-sensus protocols for IoT networks," arXiv preprint arXiv:1809.05613,2018.
[12] I. Dagan and A. Itai, "Word sense disambiguation using a second language monolingual corpus," Computational linguistics, vol. 20, no. 4, pp. 563–596, 1994.
[13] A. Outchakoucht, E. Hamza, and J. P. Leroy, "Dynamic access controlpolicy based on blockchain and machine learning for the Internet ofThings," Int. J. Adv. Comput. Sci. Appl, vol. 8, no. 7, pp. 417– 424,2
[14] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Hybrid computationoffloading in fog and cloud networks with non-orthogonal multipleaccess," in Proc. IEEE INFOCOM'18 Workshops, Apr. 2018, pp.
[15] L. Zhu, H. Dong, M. Shen, and K. Gai, "An incentive mechanismusing shapley value for blockchain-based
[16] The inside story of Mt. Gox, Bitcoin's $460 million disaster.Accessed 2018-09-07. [Online]. Available: https://www.wired.com/2014/03/bitcoin-exchange\.