International Engineering Journal For Research & Development
Vol.4
Issue 5

E-ISSN NO:-2349-0721

Impact factor : 6.03

MERGING AI WITH BLOCKCHAIN FOR SECURE ENVIRONMENT FOR DATA SHARING

Ms. Yogita S. Alone
ysalone@mitra.ac.in
Dept.Computer Science & Engg
P.R.M.I.T & R, Badnera

Dr. G.R.Bamnote
grbamnote@mitra.ac.in
Dept.Computer Science & Engg
P.R.M.I.T & R,Badner

Abstract

Artificial intelligence and blockchain are among the most problematic advancements and will on a very basic level reshape how we live, work, and collaborate. Blockchain can be profoundly financially savvy in taking out the requirement for a brought together expert to administer and check cooperations and exchanges among a few members.In blockchain, each exchange is cryptographically marked and confirmed by all mining hubs which hold a copy of the whole record which contains anchored squares all things considered. This makes a safe, synchronized and shared timestamped records that can't be adjusted. Another noticeable field that is increasing enormous footing is counterfeit intelligence(AI) which enables a machine to have intellectual capacities to learn, surmise, and adjust dependent on information it gathers.

Keywords *: Artificial Intelligence, Blockchain, Data sharing*

1.Introduction:

Blockchain is one of the driving forces in the world of technology innovation. It has revolutionized various industries including healthcare, supply chain, mobile apps, retail, real estate and finance and has added a layer of security and transparency to their processes. And along the way, it has become one of the technology transferred by entrepreneurs and their users. Artificial intelligence has also had a similar impact on the business world[3]. Technology, in the form of chatbots, has revived traditional businesses and advanced the customer experience. It has established itself as a core part of every business, be it finance, travel, retail, health, real estate, or mobile apps. Any blockchain and AI have laid the foundation for a new business era in one way or another. But have you ever thought about what will happen when the two technologies meet? Will their co-existence fit into the industry? Will they improve the economy or make it worse? Before digging deeper on how the fusion of the two technologies will unfold and how it will change the face of businesses, let's take a look at what blockchain and AI value in the current market [4].

1.1. Artificial intelligence:

Artificial intelligence (AI) is the simulation of human intelligence processes by machines, especially computer systems. These processes include learning (acquisition of information and rules to use information), reasoning (using rules to reach predictable or definitive conclusions), and self-improvement. Special applications of AI include expert systems, speech recognition, and machine vision[5]. AI can be classified as weak or strong. Weak AI, also known as narrow AI, is an AI system that is designed and trained for a particular task. Virtual personal assistants, such as Apple's Siri, are a form of weak AI[9]. Robust AI, also known as artificial general intelligence, is an AI system with generalized

human cognitive abilities. When presented with an unfamiliar task, a robust AI system is capable of finding a solution without human intervention. Because hardware, software, and staffing costs for AI can be expensive, many vendors incorporate AI components into their standard offerings, as well as access to artificial intelligence as a service (AIaaS) platform. Artificial intelligence is the technology that makes machines smart to imitate human intelligence and act on their own[7].

1.2 Blockchain: A new technology called blockchain promised greater transparency, increased security, efficiency, speed, and lower costs. The first blockchain - bitcoin - entered the public after the 2008 financial crisis. Blockchain, in common language, is a distributed ledger that stores all transactions in nodes in a transparent and secure manner[12].

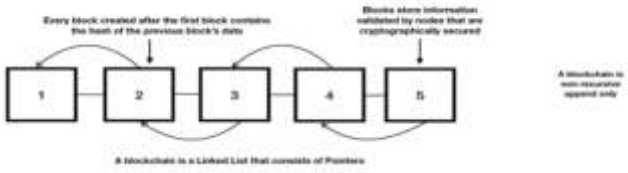

Figure 1.2.1: Block link in Blockchain

1.3. Data sharing approaches: All this raises important questions as to what type of data sharing approach is needed for AI & ML to work successfully.

a). Publish the data into a domain specific public research platform: based on key data types and uses (chemistry and assay data, pharmacological, imaging) that support direct submission. PubChem, ChEMBL, Protein Data Bank (PDB), Cancer Imaging Archive.

Figure 1.3.1: Publish the data into a domain specific public research platform

b) Publish the data into a broad domain agnostic public research repository: This could include publishing to a journal or preprint server (e.g bioRxiv, chemRxiv) at the same time as the data submission (e.g. Figshare , Zenodo). Ability to extract data & metadata from the submitted datafile depends a lot on the quality of the original submission and its structured nature

c)Use a Trusted partner or data consortium: Establish a trusted partner or consortium/alliance model who will store the data and make it accessible according to agreed rules among the partners with rules on access both for the data depositors and also for data access & analysis in general.

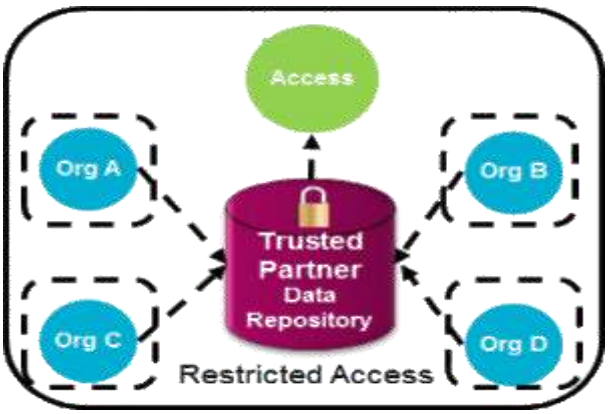

Figure 1.3.2 – Trusted Partner

d) Point to point data sharing:

A variation of the trusted partner model for when two organisations wish to share with each otherThere may be issues and restrictions with what data can be shared as with the trusted partner model.

1.4. AI Model Building Implications for data sharing scenarios:

It will be important to create models for data from different organizations, where datasets of an organization's work are not sufficient to create a representative model that has wide applicability. We will need to work on solutions that support data sharing preserving privacy that allow the model to be developed and refined and we discuss some of these. Each of these data sharing approaches has different implications for the AI model that can be derived. The Open Minded community is also looking into this.1.Public Data Repository or Publication: For public data repository or publication, one then uses the data and constructs the model. The key here remains the quality and metadata associated with the dataset.

2. Reliable Partner and Model Building: Models must be manufactured by a trusted partner in a reliable environment. This is the simplest approach to model construction compared to the ones described later. It follows the model of Lhasa.

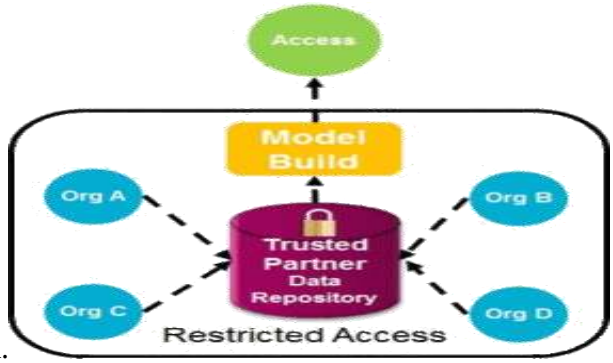

Figure 1.4.1: Trusted Partner Model Build in AI

3. Privacy-preserving (Federated Model Building):An extension of the trusted partner model using a technical solution that takes the model-building process to the data in each of the locations/organizations that the data exists[20].

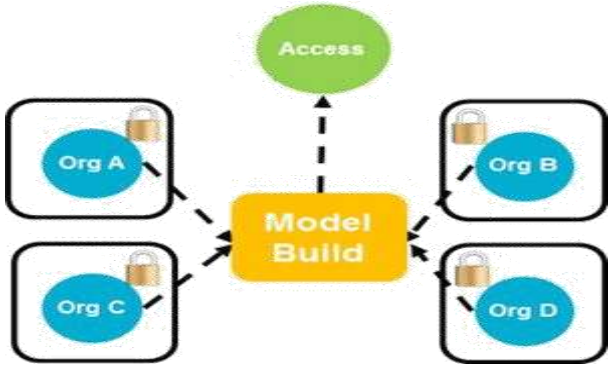

Figure 1.4.2 : Federated Model Build

1.5 AI and Blockchain Merger:

Fundamentally, blockchain is concerned with keeping accurate records, authentication, and execution while AI helps in decision making, assessing and understanding certain patterns and datasets, ultimately enhancing autonomous interactions[15]. AI and blockchain share many features that will ensure a seamless connectivity in the near future. AI is one of the most special trends in the world of modern technology[16]. But in most cases, businesses are not able to implement more interpretive AI applications. Any blockchain and AI is able to influence and influence data in a different way, making it a golden combination. This combination can bring data insights to a whole new level to provide deeper and more accurate insights. The blockchain is particularly useful for acting as an access layer and offers the performance requirements necessary for AI to be able to process data[19].

a) AI and blockchain require data sharing: A decentralized database emphasizes the importance of sharing data between multiple customers on a particular network[22]. Similarly, AI Big Data, in particular, relies heavily on data sharing. With more open data to analyze, the forecasting and estimation of machines are considered more accurate, and the algorithms generated are more reliable. Any AI and blockchain differ conceptually[23]. AI is centralized and its result is based on probability. Intermittent block-boxes (complex algorithm processes) that sit between input and output usually do not appear. But, data in a blockchain is decentralized and transparent. The data in a blockchain is secure and cannot be changed due to the cryptography involved[18]. All the data in the blockchain ledger is stamped with time. Data is distributed between participants or nodes. AI and blockchain can help each other in achieving better results.

b) Security: There is a great need for security when dealing with high value transactions on the blockchain network. It is implemented through existing protocols. For artificial intelligence, the autonomous nature of machines also requires a high degree of security to reduce the likelihood of a catastrophic event. AI relies on the correct data to correct its algorithm and end result. Blockchain helps to secure data without any tampering. The data in the blockchain is encrypted in such a way that it cannot be changed or altered. This secure data means better AI models and better results. With clearly organized data, blockchain enables new markets for transparent data trading. Thus, it can help[14].

C) Trust is a requirement: There is no greater threat to the progress of any widely accepted technology than lack of trust and neither AI nor blockchain is excluded. To facilitate machine-to-machine communication,

there is an expected level of trust. To execute certain transactions on a blockchain network, trust is required. Trust is the foundation of every business relationship. Success builds on this, and is part of how we take care of our business network. We also use middlemen in our relationships, and they instill trust and we should have trust. Banks ensure that we treat the right counterparts and that the transactions are in the right quantity. We control lawyers not to copy or distribute our products illegally. Overall, the use of middlemen is very complex, it costs a lot of time and money, and in this era of hackers, it also poses security risks. A key point is that the documentation is not only managed in one location, such as the bank's central server, but it is distributed among users of the blockchain. There are countless copies, possibly millions distributed throughout the network. Blocking of the blocks ensures that the contents of the block remain reliable at all times. For example, if a change is recorded in a block, such as a payment statement, all computers in the entire network check the blockchain to see if the transaction was valid. By combining encryption, decentralization, multiple stakeholders and community control, the system is almost impossible for hackers to penetrate. Trust arises not from between parties or through an intermediary but from a process of comparison across technology and networks. Don and Alex Tapscott, who recently wrote a book on the subject, called the blockchain a "trust protocol", a broader data access and an improved data monetization model.

Conclusion:

In order to leverage AI and blockchain to fit the problem of abusing data, as well as empower AI with the help of blockchain for trusted data management in trust-less environment. AI-based secure computing platform as well as blockchain based incentive mechanism, offering paradigm and incentives for data merging and more powerful AI to finally achieve better network security.

References

[1] J. G. Andrews, S. Buzzi, C.Wan, et al. What will 5G be [J]. IEEE Journal on Selected Areas in Communications, 2014, 32(6): 1065-1082.

[2] T. Li, Z. Xiao, H. M. Georges, et al. Performance analysis of co- and cross-tier device-to-device communication underlaying macro-small cell wireless networks [J]. KSII Transactions on Internet & Information Systems, 2016, 10(4): 1481-500.

[3] X. Foukas, G. Patounas, A. Elmokashfi, et al. Network slicing in 5G: Survey and challenges [J]. IEEE Communications Magazine, 2017,55(5): 94-100.

[4] M. G. Kibria, K. Nguyen, G. P. Villardi, et al. Big data analytics, machine learning and artificial intelligence in next-generation wireless networks [J]. IEEE Access, 2018, 6: 32328-32338.

[5] I. Chih-Lin, Q. Sun, Z. Liu, et al. The big-data-driven intelligent wireless network: Architecture, use cases, solutions, and future trends [J]. IEEE Vehicular Technology Magazine, 2017, 12(4): 20-29.

[6] F. Chiti, R. Fantacci, M. Loreti, et al. Context-aware wireless mobile autonomic computing and communications: Research trends and emerging applications [J]. IEEE Wireless Communications, 2016, 23(2): 86-92.

[7] R. Li, Z. Zhao, X. Zhou, et al. Intelligent 5G: When cellular networks meet artificial intelligence [J]. IEEE Wireless Communications, 2017, 24(5): 175-183.

[8] C. Dincer, E. Zeydan. Big data security: Requirements, challenges and preservation of private data inside mobile operators [C]//IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Istanbul, 2017: 1-6.

[9] P. Domingos. A few useful things to know about machine learning [J]. Communications of the ACM, 2012, 55(10): 78-87.

[10] G. P. Kumar, P. Venkataram. Artificial intelligence approaches to network management: Recent advances and a survey [J]. Computer Communications, 1997, 20(15): 1313-1322.

[11] A. Hintze. Understanding the four types of AI, from reactive robots to self-aware beings [J]. The Observer, 2016.

[12] G. P. Kumar, G. P. Babu. Optimal network partitioning for fault tolerant network management using evolutionary programming [J]. Information Processing Letters, 1994, 50(3): 145-149.

[13] H. E. Rauch, T.Winarske. Neural networks for routing communication traffic [J]. IEEE Control Systems Magazine, 1988, 8(2): 26-31.

[14] X. Cheng, L. Fang, L. Yang, et al. Mobile big data: the fuel for datadriven wireless [J]. IEEE Internet of Things Journal, 2017, 4(5): 1489- 1516.

[15] D. Naboulsi, M. Fiore, S. Ribot, et al. Large-scale mobile traffic analysis: a survey [J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 124-161.

[16] S. Huang, Q. Liu, T. Han, et al. Data-driven network optimization in ultra-dense radio access networks [C]//2017 IEEE Global Communications Conference, Singapore, 2017.

[17] C. Zhang, H. Zhang, D. Yuan, et al. Citywide cellular traffic prediction based on densely connected convolutional neural networks [J]. IEEE Communications Letters, 2018, 22(8): 1656-1659.

[18] G. Cao, Z. Lu, X. Wen, et al. AIF: An artificial intelligence framework for smart wireless network management [J]. IEEE Communications Letters, 2018, 22(2): 400-404.

[19] B. S. Nakamoto. A peer-to-peer electronic cash system [J]. 2008.

[20] W. G. Ethereum. A secure decentralised generalised transaction ledger [J]. Ethereum project yellow paper, 2014, 151: 1-32.

[21] T. Swanson. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems [J]. Report, available online, 2015.

[22] E. Androulaki, A. Barger, V. Bortnikov, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains [C]//13th EuroSys Conference, Porto, 2018: 30.

[23] M. Castro, B. Liskov. Practical Byzantine fault tolerance and proactive recovery [J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

[24] A. Azaria, A. Ekblaw, T. Vieira, et al. Medrec: Using blockchain for medical data access and permission management [C]//IEEE International Conference on Big Data, Washington D. C., 2016: 25-30.

[25] A. Dubovitskaya, Z. Xu, S. Ryu, et al. Secure and trustable electronic medical records sharing using blockchain [J]. arXiv:1709.06528, 2017.