iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44142

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Application of Blockchain in Artificial Intelligence

Saima Khan[1], Omprakash Mangde[2]
[1, 2]*MET Institute of Computer Science*

Abstract: ***Artificial intelligence (AI) refers to the simulation of human intelligence in machines designed in such a way that machines can think like humans and imitate their actions. It combines sub-fields for machine learning and in-depth learning, using data-trained AI algorithms to make predictions or categories, and become smarter over time. The benefits of AI include automated repetitive tasks, improved decision-making and better customer experience. Blockchain is a shared, unchanging platform that provides fast, shared and transparent data exchange at the same time across multiple groups as they begin and complete transactions. The blockchain network can track orders, payments, accounts, production, and more. Because members are allowed to share a common vision, they gain confidence and trust in their work and other businesses, as well as new efficiency and opportunities. AI can successfully mine with a large database and create new environments and discover patterns based on data behaviour. Blockchain helps to effectively remove bugs and counterfeit data sets. The two technologies complement each other as Blockchain can reduce the risk to AI, and AI can improve Blockchain performance. Much research is currently being done on the use of Blockchains to detect intelligent applications in key areas such as health care, finance, power, government, and defense.***

I. INTRODUCTION

AI and blockchain seem to be a powerful combination, enhancing almost every industry in which it is used. Blockchain and artificial intelligence combine to improve everything from providing food supply and sharing health care records to media benefits and financial security. The integration of AI with Blockchain affects many aspects, including Security - AI and blockchain will provide a double shield against cyber-attacks. The two technologies have the same requirements for data analysis, security, and trust, and can empower each other. For example, artificial intelligence is based on three key elements: algorithms, computer capabilities, and data, and the blockchain can break a data island and detect the flow of algorithms, computer capabilities, and data resources, based on its natural features, including distribution, consistency, and anonymity.. In addition, the blockchain can ensure the integrity of the original data as well as the reliability of the research and the follow-up of the performance intelligence. In addition, the blockchain can record artificial intelligence decisions, which help to analyse and understand artificial intelligence behaviours and ultimately promote artificial intelligence decisions, making them transparent, descriptive, and reliable. Artificial intelligence can improve blockchain design to make it more secure, energy efficient, and efficient. There is an increase in online attacks such as identity theft, data breach, etc. There are various security measures online to deal with such types of attacks. Blockchain technology is a trend that emerges in the online and digital world, providing high security. Available security measures are based on centralized servers / systems. Here, the empty points of failure, the risk of security breaches, and the need for trusted foreign companies are all bad. Instead, Blockchain technology is a system divided into an area where there are no reliable third parties, and trust is established within the nodes available on the network.

II. APPLICATION AREAS OF BLOCKCHAIN IN AI

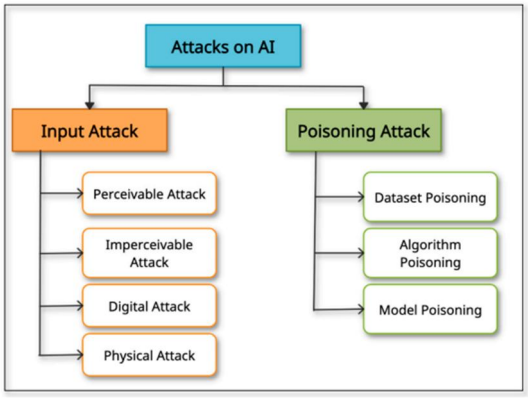
A. Blockchain AI-based Healthcare Application

Many health care organizations do not want to share their data with third party companies that process privacy issues. This makes it difficult to build a robust AI model and use it in real-time environments when patient data is split between different users. Then it will not be easy to build a standard prediction model. Therefore, to solve this problem, Blockchain can be integrated with AI to protect data access and prevent the implementation of integrated learning applications in health care applications. With smart agreements, access control rules will be put in place for access to data from different data managers for secure data sharing.

B. Blockchain for AI Application Protection

Input attacks are those where input in the AI System is modified to change output, as in the case of a distorted image. You do not need to have a corrupt AI system. Input attacks fall into four categories: visual, virtual, digital and physical attacks. Visual attacks are those that are present in the body organs and are visible to the human eye. Attacks on physical or digital organizations that are invisible to human senses are known as invisible attacks.

Digital attacks are carried out on digital data such as photos, videos, documents, and files and are often invisible. In the case of physical assault, the target is material. In most cases, physical attacks are simple and obvious. In a toxic attack, the attacker intends to damage the AI model so that when used, it has a natural vulnerability that makes it easy to control. Database learning algorithms learn model by identifying patterns in toxic data, leading to disruption of the learning process. Cheating algorithm by identifying weaknesses in it is known as algorithm poisoning.



Cybercriminal criminals disrupt blockchains in four ways: identity theft, traffic, Sybil, and 51 percent attack. Identity theft is a fraudulent way to obtain user information. Gaining access to user information and other sensitive information may result in the loss of both the individual and the blockchain network. Blockchains rely on real-time data transfer. Data may be monitored while forwarding to Internet service providers by attackers. In the Sybil attack, cybercriminals create and use many fake network identities to hack the network and destroy the system. Mining, especially in large public blockchains, requires a lot of computing power. The miner or miners' team, on the other hand, may control more than 50% of the mining power in the blockchain network if they combine sufficient resources. Controlling the ledger and having the ability to change it gives you more than half the power. Private blockchains, on the other hand, are protected from 51 percent attack.

III. ANALYSIS

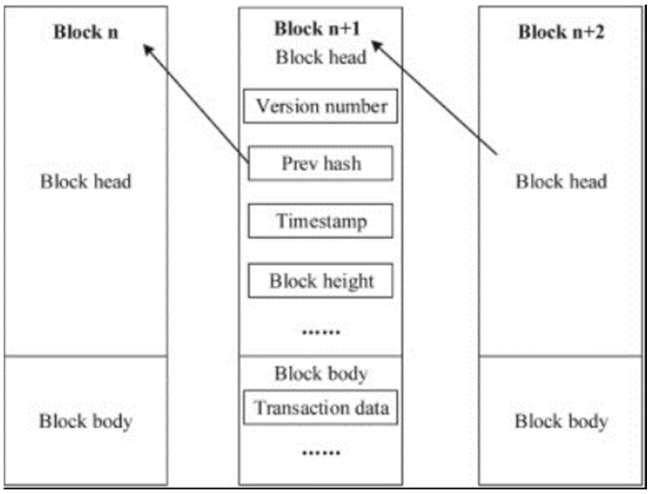
Blockchain has been described as the fifth most disruptive computer paradigm behind the main framework, personal computer, the Internet, and mobile and social networking. Because the nodes in the blockchain follow the same accounting and compliance rules under the consensus algorithm, adopt a one-way hash algorithm, and consistently produce blocks in chronological order, blockchain has the advantages of consistency and encryption protection. Currently, there are four major security and privacy issues in the blockchain. First, to successfully solve the problem of sustainable income for miners, the blockchain helps miners co-operate in mining by creating mines in the mines. However, the invaders began attacking the mines in the mine to improve their income. For example, on May 22, 2018, hackers began a 51% attack on blockchain Verge, successfully seizing approximately 35 million anonymous coins. On January 5, 2019, hackers began a 51% attack on the old blockchain Ethereum (ETC) by leasing computer imagery, which cost $ 1.1 million. Second, because the blockchain peer-to-peer network must maintain timely communication between nodes, attackers begin to attack network communications in the blockchain, which severely affects network performance and significantly reduces communication efficiency among miners. For example, on September 22, 2016, hackers launched a denial-of-service (DDoS) distribution on the Ethereum (ETH) blockchain, which significantly reduced its network performance, resulting in two strong ETH forks.

Third, although smart contracts improve the usability and flexibility of blockchain applications, some loopholes still exist in the process. By identifying these threats, the attackers launch a smart contract attack and steal huge revenues. For example, on June 17, 2016, hackers exploited the smart contract of a decentralized autonomous organization (DAO) to obtain more than 3 million illegal ETH benefits, eventually forcing ETH into a solid fork.

A. Blockchain Feature and Structure

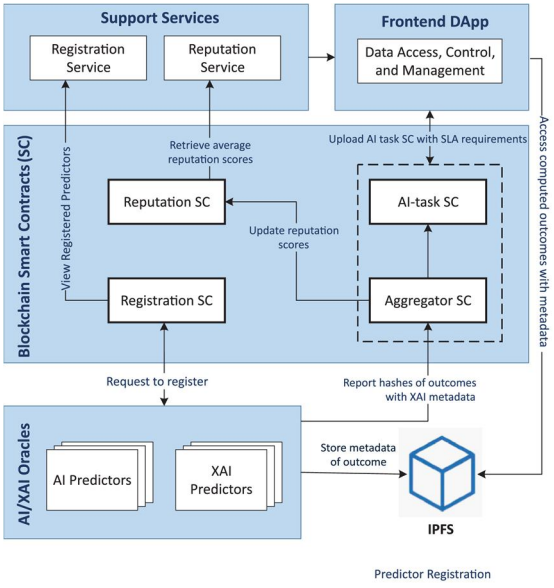
Blockchain is a new integrated design that integrates computer technologies, such as distributed data storage, networks, compatibility algorithms, and encryption algorithms. It is a type of series sequential data structure, which ensures the stability of a distributed ladder using cryptography.

Block structure: Each block has two parts: a blockhead and a block body. Blockhead contains version number, previous block hash value, timestamp, and block length. The block body records transaction block data.



IV. PROPOSED DESIGN

Explanatory and reliable AI Blockchain: Attack of AI applications is not the same as cyber-attacks. Rather, this is a deliberate deception or a distortion of the data or model level. Ultimately, the goal is to make AI applications less efficient. Because of its transparency, privacy, consistency, security, and privacy features, Blockchain, as a spatial division, offers AI data management benefits. The platform was developed using intelligent Blockchain contracts to record, control interactions and provide AI predictive compatibility and results between AI and XAI Oracles to achieve descriptive and reliable AI.



V. IMPLEMENTATION

A. Step 1: Vision

There is a need for new ways and solutions to attack inputs into AI systems and create robust AI. As data is used through weapons, we need advanced and secure strategies to collect, store, and process data. Because of its transparency, privacy, consistency, security, and privacy features, Blockchain, as a spatial framework, offers AI data management benefits. All transactions for accessing AI databases can be recorded in Blockchain for consistent research.

B. Step 2: How to Improve

1) When an attacker imitates multiple people at once, this is known as Sybil's attack. As a result, when you connect to a P2P network, this becomes a major problem. In order to participate in the mining process, each site must solve a complex cryptographic puzzle. It is still possible to increase ownership but owning a computer solution for complex issues is difficult. With the addition of leading zeros, the Cryptographic problem becomes more complex. Therefore, PoW is a balanced way to combat Sybil attacks during mining.

2) A blocked access control framework can significantly reduce data toxicity attacks in the IoE area. Data can be safely transferred within fog servers and IoT smart devices.

3) A widely distributed secure model can be set up to share Cyber intelligence between different participants using Blockchain technology. It will ensure that electronic records are uninterrupted and consistent use by smart contractors.

4) Malware injection attacks (e.g., Ransomware attacks) are network attacks that begin to encrypt sensitive files, resulting in abnormal behaviour on its system or unexpected system shutdown. To save files or activate the program, you need a configuration key that will be paid for using it. With the blockchain block chain and its feature of proof of disruption, a consortium Blockchain was introduced on the IoT network to address this security issue.

5) Powerful devices can be blocked from accessing the server by connecting IoT and Ethereum. Device sharing of device resources can deal with DDoS attacks.

6) Secure Learning Chain (SLC) is a framework designed to protect distributed machine learning using an approved Blockchain. To protect against malicious central servers, also the Identifiable Practical Byzantine Fault Tolerance (IPBFT) algorithm can be used. This algorithm can also be used to detect malicious central servers and make communication easier.

7) Smart blockchain technology ensures chain data transparency through full node ledger synchronization and ensures data tracking using transaction signatures and time stamps and more after certification. A transparent and reliable information sharing channel has been built among many participants.

8) Blockchain recognizes the expansion of computing capacity through its expanded environment, which is useful for seeing the performance of intelligent performance models in segregated global nodes and in recognizing shared computing.

9) One of the challenges faced in a reliable AI application is Bias and counter-attacks on AI use can be toxic to learning processes and guidelines. The solution is to use the blockchain platform IBFS, the definition is researched in a consistent, uninterrupted, distributed, and traceable way with high reliability and robustness. This will make the XAI system stronger, more reliable, and capable of reducing discrimination and attacks on your opponents.

10) In the AI-based Healthcare Application there is a problem of privacy concerns in sharing health care records with third parties to make the AI model even higher.

Strength and difficulty in building a standardized speculation model for fragmented data. This can be solved using Blockchain - a smart contract by establishing rules to control access to a smart contract for creating personal health care records. This helps to build robust AI models and share personal health care records without compromising.

VI. CONCLUSION

Blockchain technology is not just about financial transactions or cryptocurrencies. Instead, Blockchain is seen as an emerging technology for accessing important applications. Some technologies have a level of complexity, but both Blockchain and AI are in situations where they can benefit and help each other. The integration of machine learning and AI into blockchain, and vice versa, can improve Blockchain's basic structures and increase AI capabilities, respectively. In this case, the focus is on Blockchain to protect AI and unlock new ones. It can make AI more consistent and understandable, and we can track and determine why decisions are made on learning models and how reliable they are. Blockchain and its ledger can record all data and decision-making changes under AI models. AI can securely access various data via Blockchain while maintaining the privacy of data and data providers.

In-depth learning models can work more efficiently and accurately when trained with big data. In the case of health care applications, having big data in one place is a challenge. Data from various hospitals, laboratories, and research institutes can be used collaboratively to train in-depth learning models. However, confidentiality is a major problem, limiting the sharing of medical data within different organizations. The development of in-depth learning models with Blockchain is the solution to this type of problem. Since Blockchain itself has its own limitations, all data cannot be added to Blockchain. It stores and shares only the weights of a locally trained model in isolated areas using smart contracts, enabling Blockchain-divided networks to train a global model. In some cases, all data access activities for in-depth learning models can be recorded in Blockchain. With smart contracts, it can use access control rules to avoid data misuse.

Learning algorithms and information testing can be done automatically based on network status due to smart contracts embedded in the blockchain. To balance and monitor the channel, Blockchain can also maintain active search tracks and permanent shortcuts and stability, which will improve search strategies for different applications.

In the event of a catastrophic failure of AI-based applications, administrators may research descriptions generated by descriptive AI. However, these definitions are stored on intermediate servers. They do not provide security and tracking so that the owner can tamper with the data. Blockchain can overcome these security restrictions. IPFS can store all of these definitions, and those can be restored to descriptions, and those can be found in the Ethereum blockchain. Storing and retrieving descriptions can be done with a smart contract. AI applications can benefit from Blockchain features such as consistency, transparency, privacy, trust, and security.

VII. FUTURE WORK

We are on the verge of a blockchain-driven social media platform. However, before the distribution of social media can reach its full potential, disrupt the power of hate-loving social giants and become the next big thing, more efficiency and technology need to be developed.

Adding more activities such as integration and improving public trading opportunities

Creating smart contracts that include Digital rights, wagers and escrow on scattered social media networks.

It should start with wearable items such as virtual reality, and then move on to blockchain-enabled social media platforms.

literature review

The global blockchain AI market is expected to grow from $ 297.62 million by 2021 to $ 384.44 million by 2022 with a combined annual growth rate (CAGR) of 29.2%. The change in growth is mainly due to the companies that are stabilizing their production after meeting the growing demand during the COVID-19 violence in 2021. The market is expected to reach $ 934.45 million by 2026 at the CAGR of 24.9%.

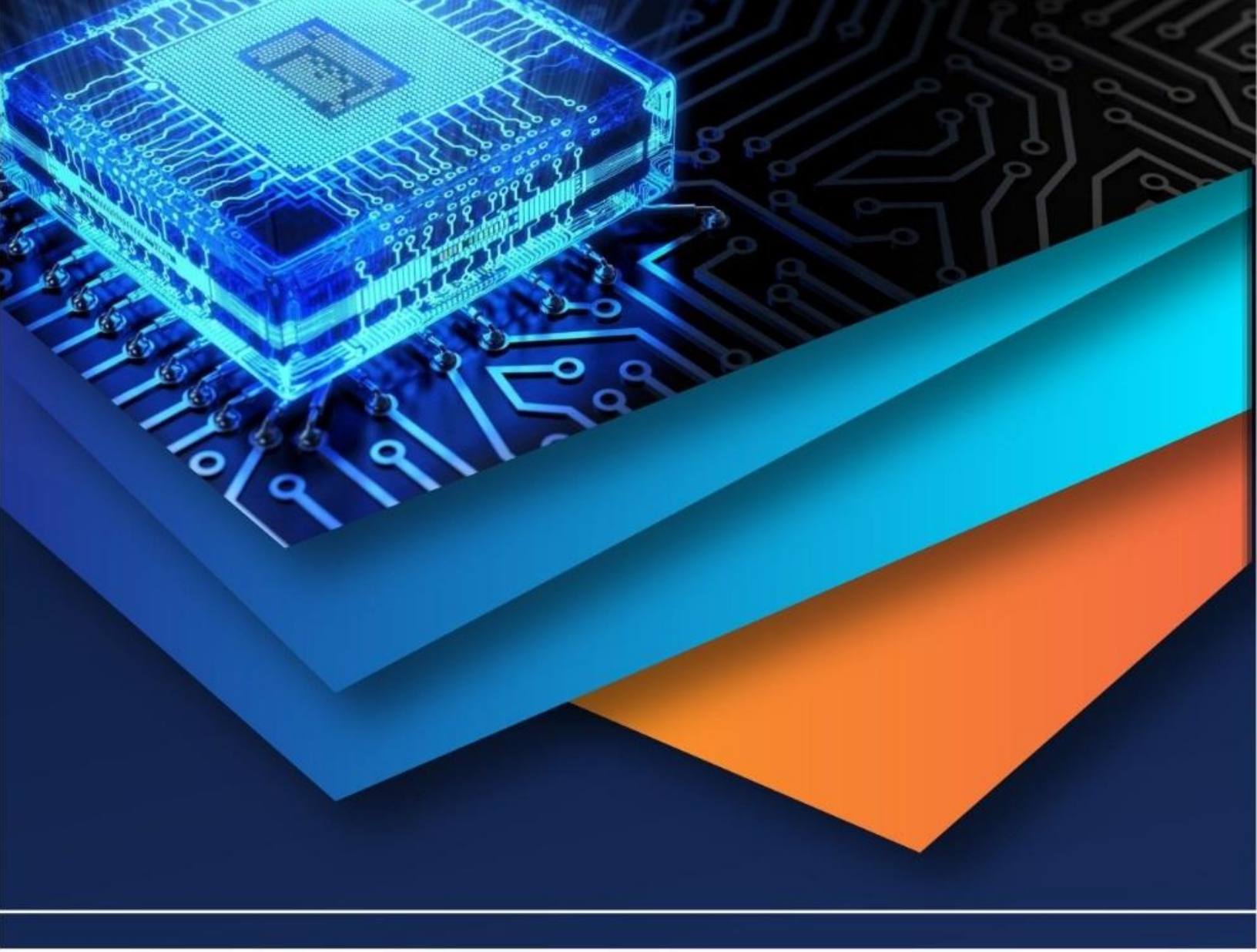
The blockchain AI market consists of the sale of blockchain AI technology and related services (organizations, sole vendors and relationships) that provide blockchain and AI technology. Blockchain is a universally distributed computer network that records and stores data to display a sequence of events in a transparent and unchangeable layout system.

North America was the largest blockchain AI market in 2021. Asia Pacific is expected to be the fastest growing region in the forecast period. The regions included in the report are Asia-Pacific, Western Europe, Eastern Europe, North America, South America, the Middle East and Africa. Blockchain technology, in particular, has shown great potential when combined with the performance of a learning machine.

According to a study by O'Reilly in 2019, 85% of 1,388 organizations use AI in production. Many companies that used to try to use AI are now moving forward and implementing it in this process. Therefore, investing in blockchain technology by enterprise businesses plays a major role in business success. In June 2020, NetObjex acquired Vital Grid for an undisclosed price. The agreement will expand NetObjex's Digital Transformation product and services. NetObjex is an Operating Platform for Digital Assets using artificial intelligence, Blockchain and IoT with applications in Manufacturing, Supply Chain, Transportation and Smart Cities. Vital Grid provides business expertise and consultation with management to improve performance, simplicity processes and risk reduction by delivering technology-enabled business transformation.

REFERENCES

[1] Blockchain for explainable and trustworthy artificial intelligence https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1340
[2] Blockchain and AI https://www.ibm.com/topics/blockchain-ai#:~:text=By%20providing%20access%20to%20large,trustworthy%20and%20transparent%20data%20economy.
[3] Blockchain AI Global Market Report https://www.thebusinessresearchcompany.com/report/blockchain-ai-global-market-report
[4] Approaches of Blockchain with AI: Challenges & Future Direction
[5] Practical Artificial Intelligence and Blockchain by Ganesh Prasad Kumble, Anantha Krishnan



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY