# Assessing the Safety of Blockchain Technology in the Emerging AI Era

**[1]Akash Verma, [2]Ratnesh Kumar Pandey,[3]Jaychand,**

[1]Pursuing Masters in Technology, Department of Computer Science,
[2]Associate Professor, Department of Computer Science,
[3]Ph.D Scholar, Department of Computer Science,
[3]Assistant Professor, Department of Computer Science,
[1 2 3]Invertis University, Bareilly, Uttar Pradesh, India,
[3]Kamla Nehru Institute of Physical and Social Sciences Faridipur Sultanpur U.P. India
Email Id: [1]dverma765@gmail.com, [2]itmcse.rp@gmail.com, [3]jaychandvbs04@gmail.com

**Abstract**: Blockchain technology has garnered significant attention in recent years due to its potential to revolutionize various industries, including finance, supply chain management, and healthcare. Simultaneously, the rapid advancement of artificial intelligence (AI) technologies is reshaping how businesses operate and interact with data. This paper examines the safety considerations of integrating blockchain technology with AI systems. We explore the potential benefits and challenges of this integration and evaluate the security implications of using blockchain in the context of AI-driven applications. Through a comprehensive analysis, we aim to provide insights into the safety of blockchain technology in the forthcoming AI era.

**Keywords**: Blockchain, Artificial Intelligence, Security, Privacy, Integration, Smart Contracts, Supply Chain, Data Integrity.

## I. Introduction:

The convergence of blockchain technology and artificial intelligence represents a promising frontier in innovation. Blockchain, originally devised for secure and transparent transactions in cryptocurrencies, has evolved into a versatile tool with applications in data management, authentication, and decentralized governance. Meanwhile, AI technologies, powered by machine learning algorithms, have demonstrated remarkable capabilities in data analysis, pattern recognition, and decision-making. The integration of these two technologies holds the potential to address various challenges related to data integrity, transparency, and trust in AI systems. However, concerns regarding the safety and security of blockchain in the context of AI implementation remain a subject of debate. Blockchain, and Artificial Intelligence imitate extraordinary chances for the public sector and business sector. Unification of these two technologies

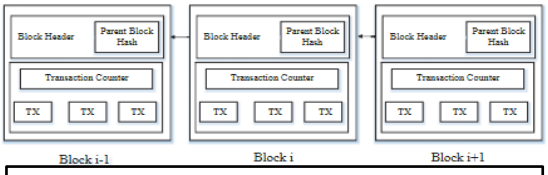



Figure 1. Visualization of Blockchain

equip predictive methods, share data from one device to another with privacy and security, and solve neurons regarding problems and share data resources between machines. Each and every field is proficient to deed these technologies through which they create new models, enhance the ongoing processes and grant services for the customers.

## II. Overview of Blockchain Technology and Artificial Intelligence:

This section provides a brief overview of blockchain technology, including its fundamental concepts, key components, and underlying principles. It discusses the decentralized nature of blockchain networks, consensus mechanisms, cryptographic techniques, and smart contracts. Additionally, it highlights the core features of blockchain, such as immutability, transparency, and traceability, which contribute to its perceived security benefits. Blockchain in simple words can be described as a data structure that records all the

transactions happening among the participants of the network in the form of blocks while ensuring decentralization, transparency, and security. Every member of the network can validate or check the data without any need for the authorization of the third party which makes the process more effective, faster, and cost-efficient. Each block in the network stores the information of the transactions, but once the data is stored in the ledger no member can tamper with it. All the data in the blockchain is stored digitally using the digital signatures and encryption algorithm that proves its authenticity and decreases the chances of leakage of data. Blockchain also makes the payment system more secure and easier for example, if you are looking to transfer some money to your relative who lives far from you. A general option that will come to your mind will be any online payment application or bank that will include the third party in order to transfer the money or make the transaction, due to which you will also have to pay the extra fee. Besides, there is no full security for your money any hacker can hack the system and seize the money. Here the blockchain enters. Using blockchain instead of the traditional banking system for the process of transferring money, can be more secure and easier. This technology excludes the need for a third-party and the transaction can directly be processed by you so there is no extra fee to pay. Block chain works upon a decentralized system means all the data stored in a blockchain is not confined to a single place, the data stored in the network is public and decentralized. Every transaction in the network is directly visible to every participant, everyone contains a copy of the distributed ledger but no one can edit the data appended in the ledger. This maintains the immutable history of every member's activity and offers the full traceability and transparency of all the transactions to everyone that ever happened in the network. Now let's understand how the blockchain technology works. In a blockchain network, every block contains the hash of the preceding block along with some information. Now a hash can be defined as a mathematical code that every block carries its own. If a block stores the modified information, the hash will also subject to the modification. These unique hash keys in the chain of blocks ensure the security in the blockchain network. There are nodes in the blockchain network that access or validate all the transactions that are taking place. In Bitcoin blockchain, there are miners that validate the transactions but in order to validate the transaction they use the proof-of-work concept. And for a valid transaction, every block needs to commit the hash of the previous block. This makes the blockchain unalterable as every modification in the chain of blocks is visible to the complete network and gets caught easily. Blockchain also provides a feature in which two or more peers can securely make an agreement or arrangement over a private network on certain activities like healthcare activity, business activity without the requirement of any third party or authority. The involved peers can be total strangers and still can make the agreement. Once the agreement is recorded in the network, it is impossible for any of the involved peers to deny, cancel or alter the agreement. To assure the validity of the agreement recorded in the network, the "mining" process is used. The data stored in the blocks are highly secured with the powerful cryptocurrency that makes sure that the transactions recorded in the network cannot be tampered or forged. This makes the blockchain a trusted platform and allows the cryptocurrency to sustain a trusted transaction network without any need for authority. Also, for the past few years, the blockchain has bee

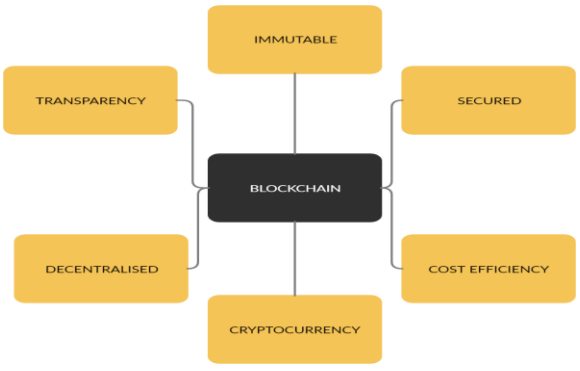
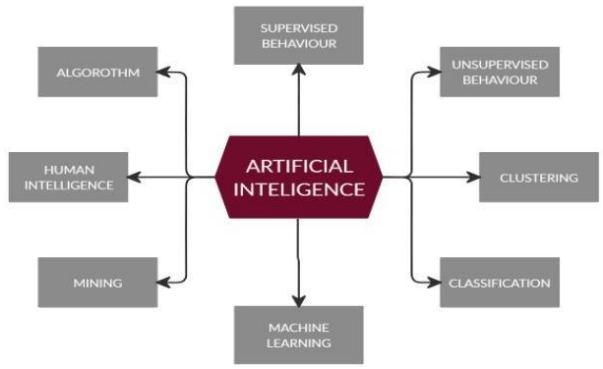



**Figure 2. Features of Blockchain**

playing a vital role in the enhancement of cryptocurrencies. Therefore, because of the enhancing properties of the blockchain, this technology is evolving very frequently and

investing the various enhancements in different fields.

Figure 3. Features of Artificial Intelligence




Artificial Intelligence (AI) is the technique to give the machines some kind of intelligence. The ability of a machine to do work without the interference of any human and also giving the machine intelligence which helps it to take decisions by itself. Various new devices are coming with this technique and this technique helps them to be more useful to humans and is increasing the demand for such new devices. Some of the few popular AI-based software and application that humans use on a daily basis are Siri, Alexa and Google Assistance. All of these software's work immediately according to the response, they get from the user. One more example of this technique is self-driving cars; Tesla Motors is one of the major manufactures of such cars and with the help of this technique the cars can literally drive themselves without and human involvement, the working of such cars take place because of the information gathering and decision making of the software. All of these AI applications are able to work because of the algorithms which are written to make such software. Various different algorithms are required for an AI device to work perfectly. Each scenario is kept in mind and algorithms are written accordingly. Artificial intelligence is of two types Centralized AI and Decentralized AI. Centralized AI can be explained as the AI technology which requires third party interference to do a task. Which means that AI technology will be under the guidance of human intelligence, humans will be required to tell what the software can do at a specific thing or a situation. Data can be tempered easily in the centralized AI and also there will be no authenticity of the software which will increase the risk of using that software to a huge extent. That is where decentralized AI is required. In decentralized AI no governed party is required to make or take decisions for the AI. The combination of AI and Blockchain together is known as decentralized AI. With the help of the Blockchain the AI can perform all the tasks without the interference of any party. So, all the analysis and decision making can be performed on a secured and private platform. Also, data tampering is not possible in a decentralized AI platform. AI and machine learning are two different techniques but they are connected to each other in a way. Machine learning is a technique that the AI software uses to take action on the tasks which are present in front of them. Now during the making and training of the AI, the learning methods that can be used are supervised learning and unsupervised learning. Supervised learning is the technique of providing the AI machine the solution for every problem that it can face. This will prepare the machine in such a way that it will already know all the problems that it can face and will have all the solutions to it. It's lengthy and detailed learning process. The second way of learning is known as an unsupervised way of learning, in this method no solution or answers are provided to the AI software. The machine is provided with a lot of data which it has to analysis itself and find the answers to the questions itself. For example, if the machine has to predict who will win the elections this year, then the machine will be provided with a lot of data related to that election and the machine will analyze it and will find a solution by itself. This is where IoT and AI are merged together because the data can be taken from an IoT device which gathers information related to it and store it in a cloud, further that cloud can be provided to the AI software for finding the results of the problem provided to them. Classification of the data according to the problem is very necessary and is done with the help of classification training given to the AI. The second important thing for

data analysis after data classification is data clustering. Data clustering is basically a process of keeping similar data together so that it can be used to find solutions related to a problem. Nowadays more and more people are opting for this technology because of the features it provides and how it is affecting human life.

## III. Advancements in AI and Data-Driven Technologies:

Here, we examine the recent advancements in AI and data-driven technologies that have propelled the adoption of machine learning, deep learning, and natural language processing algorithms. We discuss the growing reliance on AI systems for decision-making, automation, and predictive analytics across various domains, including finance, healthcare, and manufacturing. Furthermore, we explore the increasing volume and complexity of data generated by AI applications, raising concerns about data privacy, security, and integrity. Blockchain technology offers various merits and advantages across different use cases and industries.

A. Here are some of the key merits of blockchain:

**[1]. Security:**

Immutable Ledger: Once data is recorded on the blockchain, it cannot be altered or deleted without consensus from the network participants, making it highly secure against fraud and tampering. Cryptography: Strong cryptographic techniques are used to secure transactions and user identities.

**[2]. Transparency and Trust:**

Public Ledger: Public blockchains are open and transparent, allowing anyone to view transactions and data, which fosters trust and accountability. Decentralization: Decentralized networks reduce the risk of a single point of failure, making them more trustworthy.

**[3]. Data Integrity:**

Immutable Records: Data on the blockchain is timestamped and linked in a chain of blocks, ensuring the integrity and authenticity of records.

**[4]. Reduced Intermediaries:**

Peer-to-Peer Transactions: Blockchain enables direct peer-to-peer transactions, reducing the need for

intermediaries like banks or payment processors, which can lower costs and increase efficiency.

**[5]. Efficiency:**

Smart Contracts: Blockchain-based smart contracts automate and enforce contract terms, reducing manual processing, paperwork, and the risk of errors. Faster Settlement: Blockchain can facilitate quicker settlement of transactions, especially in financial markets.

**[6]. Traceability and Supply Chain Management:**

Provenance: Blockchain can track the origin and journey of products in a supply chain, helping to prevent counterfeiting and improve transparency.

**[7]. Decentralization:**

No Central Authority: Public blockchains operate without a central authority, which can reduce the risk

of censorship and control by a single entity. Censorship Resistance: Data on public blockchains is resistant to censorship, ensuring information remains accessible.

**[8]. Privacy and Control:**

User Control: Users have greater control over their personal data and who can access it, enhancing privacy.

Selective Disclosure: Users can choose to disclose only specific data to different parties, maintaining privacy while sharing necessary information.

**[9]. Cross-Border Transactions:**

Global Transactions: Blockchain facilitates cross border transactions with reduced fees and

faster processing times compared to traditional banking systems.

**[10]. Tokenization:**

Asset Digitization: Blockchain enables the tokenization of real-world assets like real estate, art, and stocks, making them more liquid and accessible.

**[11]. Innovation and Decentralized Applications (DApps):**

DApps Ecosystem: Blockchain platforms like Ethereum enable the development of decentralized applications, fostering innovation in various industries.

**[12]. Auditing and Compliance:**

Real-Time Auditing: Auditors can access blockchain data in real-time, making audits more efficient and reducing the risk of fraud.

**[13]. Resilience and Disaster Recovery:**

Redundancy: Data on a blockchain is distributed across multiple nodes, making the network resilient to failures and disasters.

**[14]. Sustainability:**

Energy Efficiency: Some blockchain networks are transitioning to more eco-friendly consensus mechanisms like Proof of Stake (PoS) to reduce energy consumption.

**[15]. Financial Inclusion:**

Access to Banking: Blockchain can provide banking services to unbanked or underbanked populations, helping to promote financial inclusion. While blockchain technology offers many merits, it also faces challenges, such as scalability issues, regulatory concerns, and the need for industry standards. The suitability of blockchain for a particular use case depends on various factors, including the specific goals, requirements, and regulatory environment of the application.

B. Introducing AI into blockchains creates new possibilities in a wide range of industries.

**[1]. Supply Chain:**

AI and blockchains are revolutionizing supply chains across sectors by adding automation and intelligence to perform transactions, making the data trustworthy and shareable, and digitizing a formerly paper-based process. Carbon emissions data can be tracked, for instance, at the product or component level, giving manufacturers more precision and insight into their decarbonization efforts.

**[2]. Financial Services:**

The introduction of trust, the elimination of friction in multi-party transactions, and the acceleration of transaction speeds are just a few ways AI and blockchains are revolutionizing the financial services business. Take the procedure of obtaining a loan for example: Applicants agree to allow blockchain access to their data. Faster closings and higher customer satisfaction may be achieved via a combination of data trust and automated application evaluation procedures.

**[3]. Life Sciences:**

The use of AI and blockchains in the pharmaceutical business has the potential to greatly increase the success rate of clinical trials while also boosting transparency and traceability across the medication supply chain. The integrity of data, automation of trial participation and data collecting, monitoring of patients, management of permission, and openness of data are all made possible by combining powerful data analysis with a decentralized framework for clinical trials.

**[4]. Healthcare:**

AI may assist in improving almost every aspect of healthcare, from bringing to light therapeutic findings and supporting user demands to recognizing insights from uncovering trends and patient data. Blockchain technology allows for the safe sharing of sensitive patient information such as electronic health records (EHR) across healthcare providers.

**IV. Integration of Blockchain and AI:**

This section explores the potential synergies and challenges associated with integrating blockchain technology with AI systems. We examine use cases where blockchain enhances the reliability, transparency, and auditability of AI-generated insights and decisions. Additionally, we discuss the role of blockchain in facilitating secure data sharing, federated learning, and model governance in distributed AI environments. Furthermore, we analyze the technical hurdles and scalability issues that may arise from combining blockchain and AI technologies. AI, automation, and blockchains may provide value to multi-party business processes by decreasing the need for human intervention, boosting throughput, and facilitating better data integrity. AI models incorporated in smart contracts implemented on a blockchain could suggest recalling expired products, reordering, paying, or purchasing stock based on predetermined thresholds and events, resolving disputes, and choosing the most environmentally friendly shipping option, among other things. AI can read, analyze, and correlate data with lightning speed and depth, giving blockchain-based business networks a competitive edge. Blockchain enables AI to expand by enabling access to enormous amounts of data from inside and outside the company, allowing for more actionable insights, better management of data consumption and model sharing, and a more transparent and trustworthy data market. By leveraging third parties, or oracles, to process the data. Using the digital record provided by blockchain technology, the AI's underlying structure and the data source it is drawing from can be better understood, thus overcoming the problem of explainable AI. Trust in data and, by extension, AI-generated suggestions is bolstered as a result. Data security may be improved when a blockchain distributes and stores AI models, particularly when combined with AI. The corporate world and bespoke software development services will see significant adoption of these two technologies over the next 5–15 years. Industry executives that are both forward-thinking and tech-savvy still see the immense potential of combining blockchains with AI.

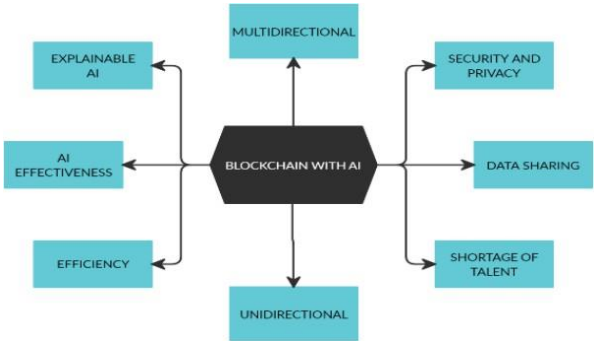



**Figure 4. Integration of Blockchain and AI**

A. Let us take a look at how one may use AI and blockchains for his or her business.

**1. Understanding How AI Thinks**

However advanced AI may be, it will never replace human judgment and hence will never be widely adopted by the public. The inability to account for the computer's actions is one of the problems that has slowed the widespread use of AI. The public will quickly come to trust AI if its decision-making processes can be recorded. Incorporating blockchain technology with AI has the potential to reveal previously hidden processes inside computers. Every AI decision may be recorded and made accessible in a distributed ledger. The information on a blockchain cannot be altered once it has been recorded, making it ideal for auditing and other security-sensitive applications.

**2. Security Improvement**

Blockchains include built-in encryption that makes the data very secure. Storing private and sensitive information such as medical records or individual recommendations on a blockchain makes a lot of sense. Continuous and massive amounts of data are essential for AI. AI algorithms that can safely process encrypted data are now the focus of intensive research and development. In any case, there is a supplementary viewpoint regarding the enhancement of security. There is a high level of security in the blockchain itself, but any extra layers or applications are not bulletproof. In the banking sector, machine learning will speed up the rollout of blockchain applications and allow for the prediction of potential system breaches.

### 3. Gaining Entry to and Control over the Data Market

This is inextricably linked to better safety measures. With the ability to store massive quantities of encrypted data on a distributed ledger and have AI efficiently manage it, fresh use cases emerge. Blockchain technology makes it possible to keep sensitive information, such as medical records, and even benefit from providing others with access to it. That's why there are now markets for data, models, and AI. Enhancing the data management processes is another advantage of integrating AI with a blockchain. To decipher encrypted data, computers go through possible character permutations until they find the one that matches the original message. A hacking AI is like a person in that it improves with practice. AI, however, will not need a human lifetime to achieve the same level of expertise. This may be accomplished fairly rapidly with sufficient training data.

### 4. Smart Contract Enhancement

Certain vulnerabilities in the blockchain's underlying technology provide a risk for malicious actors. This was very recently shown. To put it another way, smart contracts are not that smart yet. Once certain triggers are reached, they will automatically release and transfer the monies. This can only be accomplished after the blockchain community has reached a unified decision. Since the code for a smart contract is openly available, anybody may take their time to carefully examine it for vulnerabilities. The use of AI aids in the validation of smart contracts and the forecasting of exploitable flaws. Astraea, a private smart contract-based, secure, anonymous, and decentralized auditing platform for contribution systems. In particular, they combined a Distribute Smart Contract (DiSC) with an SGX Enclave to distribute contributions, demonstrate the accuracy of the gift number (intention), and protect the anonymity of donors. They created a donation smart contract by using a DiSC to reimburse deposits and protect against theft and collusion attacks from nefarious collectors and transponders. They used security reduction to explicitly describe and demonstrate Astraea's security and privacy. To carry out an in-depth performance study, they constructed a prototype of Astraea. Astraea is efficient in terms of both computing and communication, according to experimental data.

### 5. Maximizing Energy Efficiency

Energy consumption is high while data mining. This is a huge problem in the contemporary world, but Google has shown that machine learning can solve it. By feeding the DeepMind AI historical data from hundreds of sensors inside a data center, Google has enabled cutting down on the amount of energy needed to keep its data center at a comfortable temperature by 40 percent. Using this similar concept, mining hardware costs may be reduced.

### B). Security Considerations:

The security considerations of employing blockchain technology in the AI era are thoroughly examined in this section. We discuss the vulnerabilities inherent in smart contracts and decentralized applications (DApps) deployed on blockchain platforms. Moreover, we explore the potential implications of AI-generated adversarial attacks on blockchain networks and smart contracts, highlighting the need for enhanced security measures.

The integration of Artificial Intelligence (AI) with blockchain technology can yield powerful solutions that combine the strengths of both technologies.

**1). Enhanced Security:**
AI-Powered Threat Detection: AI algorithms can analyze network traffic and transaction patterns to detect and respond to security threats, enhancing the security of blockchain networks.

**2). Smart Contracts and AI:**

Smart Contract Execution: AI can be integrated with smart contracts to enable more complex and dynamic contract execution based on real-time data and events. For example, AI can trigger contract actions based on external conditions.

**3). Data Privacy and Encryption:**

Private and Secure Data Sharing: AI can be used to encrypt and securely share data on the blockchain while allowing selective access to authorized parties.

**4). Supply Chain Management:**

AI for Supply Chain Optimization: AI algorithms can analyze supply chain data stored on the blockchain to optimize logistics, predict demand, and enhance transparency in the supply chain.

**5). Identity Verification:**

AI-Driven Identity Verification: Combining blockchain's immutability with AI-powered identity verification can provide a secure and efficient way to verify individuals and entities in various applications, including Know Your Customer (KYC) processes.

**6). Tokenization of AI Models:**

AI Model Ownership and Monetization: AI models can be tokenized on the blockchain, allowing developers to sell, license, or share access to their AI models securely.

**7). Data Marketplaces:**

AI-Powered Data Marketplaces: Blockchain can facilitate data marketplaces where AI developers can access and purchase datasets for training and research.

**8). Decentralized Autonomous Organizations (DAOs):**

AI Governance in DAOs: AI algorithms can be used to assist in decision-making processes within DAOs, ensures transparency and efficiency.

**9). AI-Enhanced Prediction Markets:**

Augur is an example of a blockchain-based prediction market platform that utilizes AI and machine learning for event outcome predictions.

**10). AI-Powered Smart Oracles:**

Chain links an oracle network, is an oracle networking integrated AI-powered oracles to provide real world data to smart contracts with enhanced accuracy.

## V. Privacy and other Implications:

### A). Privacy and Security

Among the obstacles of blockchain application, privacy, security, and landing protection are major concerns. Due to its role as the backbone of the Internet of Value, the blockchain's inter-node communications are public and transparent, but they may also include sensitive data that users would like to keep secret. Therefore, the key to whether or not blockchain applications can be deployed on a big scale is how to safeguard user privacy. Typical blockchain privacy protection strategies include information concealment and identity confusion. Using privacy-protecting signature technologies such as ring signatures and group signatures to muddle the identities of both participants in a transaction, identity obfuscation technology makes it hard to match the true user to their blockchain transaction. The supervisor's private key allows the supervisor to access user data as required, protecting users' identities. The user's transaction privacy is successfully protected by information concealing, which employs technologies such as secure multiparty computing and zero-knowledge proof to complete transactions without disclosing any private information and to guarantee the credibility of the findings. The increased complexity of the calculations, however, results in a less effective system, and therefore more work has to be carried out to boost its usefulness in real-world contexts. It is not easy to figure out how to apply AI algorithms sensibly to boost inefficient performance. Furthermore, the current AI algorithm has to be redesigned to be applied to a distributed context. Private AI, which combines AI and encryption methods to solve the data security problem, was recently developed, but prior research has demonstrated that model inversion attacks may be used to reverse-engineer the

model parameters to create pictures. In this context, Khowaja et al. suggested an industrial IoT environment-specific Federated Learning and Encryption-based Private (FLEP) AI system that offers two-tier security for data and model parameters. They provided a hypothetical approach to protect the model parameters together with a three-layer encryption mechanism for data security. The suggested approach, according to experimental data, produces improved encryption quality at the cost of a somewhat longer execution time. By applying a trust-based protection mechanism, Corradini et al. suggested a two-tier blockchain architecture to improve the security and independence of smart items in the IoT. Smart items are appropriately categorized into communities in this architecture. The first-tier blockchain is local and is only used to record probing transactions carried out to assess the confidence of an item in another one of a different community or of a same community, which reduces the complexity of the solution. These transactions are periodically aggregated after a time interval, and the resulting values are kept on the secondary blockchain. In particular, the stored values are each object's standing within its community and each community's confidence in the other communities inside the framework. Moreover, the blockchain and federated learning integration method has drawn a lot of interest as a new trustworthy data-sharing pattern with privacy protection. Generally speaking, this approach bypasses the supervision of the computing process and federated learning model in favour of using blockchain technology to oversee the original data and computation outcomes. In order to create a new data privacy sharing paradigm using blockchains and federated learning, Guo et al. presented the ideas of the sandbox and state channel. They primarily addressed issues with data privacy sharing in federated learning and the deterioration of system performance brought on by poor data quality. The simulation results demonstrate that the suggested strategy outperforms and is more effective than the conventional data exchange method.

**B). Credible Oracles**

Blockchain players may trigger the execution of a smart contract by triggering an external event or calling a third-party function. Event or data retrieval automation is not a primary focus of smart contract design. To rephrase, the contracts are unable to obtain information from the real world. The contracts need to be "pushed" data and events. To address these issues, it is recommended to employ trustworthy oracles, which are essentially trusted external parties or nodes, to transmit events and data to smart contracts. When it comes to maintaining trust, oracles provide a new layer of complexity and potential security risks, as a previously decentralized system becomes centered on a set of oracles that must be relied upon. Usually, the agreement is reached by a vote among reliable oracles.

**C). Concerning the Security of Smart Contracts and the Implications of Their Deterministic Execution.**

The success of a smart contract relies on its implementation being safe against hacks and errors. Code and data on the network should be protected against intrusion wherever possible. For instance, in 2016, hackers exploited a critical flaw in the coding of the Ethereum platform used to create the smart contract for the DAO. There was a loss of 3.6 million Ethers as a consequence of this. This problem, introduced by smart contract programming and other blockchain-based applications, calls for blockchain engineering. Problems with security in smart contracts may be traced back to careless coding in the languages used to create them. The relevance of vulnerability testing for smart contracts has grown, and as a result, several tools have been created to evaluate the safety of a contract's source code. Moreover, as it stands right now, there is no such thing as a probabilistic result for the execution of a smart contract. When AI and machine learning-based decision-making algorithms are implemented as smart contracts by the mining nodes, the execution output is typically not deterministic but rather random, unpredictable, and approximative. This may be a significant difficulty for decentralized AI. With data input that might be rapidly changing as much as that of IoT and sensory readings, this calls for a

unique approach to deal with approximation computation and to design consensus protocols for mining nodes for agreeing on outputs with a certain degree of confidence, accuracy, or precision.

**D). Scalability**

The key to the successful rollout of smart blockchain applications is in solving the scalability problem. Blockchain decentralized applications need the underlying blockchain platform to function. If the scalability and performance of the system are inadequate, it cannot be deployed as a large-scale application. The blockchain's scaling concerns may be broken down into three primary categories: consistency problems, network latency, and performance constraints. Most nodes need to agree on the transaction data to guarantee the blockchain's security. The blockchain will split if the need for consistency in the distributed network is neglected in favour of faster growth. Due to its decentralized nature, blockchain's scalability is limited by the time it takes for data to travel between nodes in the network. This is particularly true for longer delays. The key problem that prevents the widespread use of blockchain applications is the impact of transaction performance on scalability. To maintain security and ultimate consistency, blockchain transactions cannot be completed in parallel, which makes it impossible to boost transaction throughput.

**E). Off-Chain and On-Chain Storage Data Cooperation**

Blockchain technologies and conventional information storage methods both have advantages and disadvantages. Both conventional information systems and blockchains require off-chain storage and compute infrastructure to boost performance. To accomplish this, it is necessary to combine blockchain technology with conventional information systems, with the most important consideration being to guarantee the accuracy and consistency of both the data on the chain and the data that are stored in conventional databases. More importantly, data are essential to the advancement of AI. There are still several obstacles to the widespread use of AI, such as issues with data quality, data monopolization, and data abuse. The introduction of blockchain technology opens up new avenues for solving these issues. The combination of blockchains and AI is only useful in the real economy if the data on the chain are properly combined with the data off the chain. In order to enable model sharing and ensure a fair model-money exchanging process between independent developers and ML-as-a-Service (MLaaS) providers, Weng et al. developed a model marketplace dubbed Golden Grain. To encourage the loyal contributions of well-trained models, they implemented the swapping process on the blockchain and subsequently created a blockchain-enabled model benchmarking procedure for openly deciding the model values in accordance with their real-world performances. Their marketplace carefully offloads the laborious computation and designs a protected off-chain on-chain interaction protocol based on a Trusted Execution Environment (TEE), for guaranteeing both the integrity and authenticity of benchmarking, particularly to reduce the blockchain overhead for model benchmarking. In order to show the realistically inexpensive performance of their architecture, they deployed a prototype of Golden Grain on the Ethereum blockchain and carry out comprehensive testing using common benchmark datasets.

**VI. Future Challenges and Conclusion:**

In this section we will discuss about the challenges faced by the unification of the Blockchain with Artificial Intelligence.

**A. Fog Computing Paradigm**

This property is newly expatiating which allows localized computing of the data that is created by the IoT devices or the customers. These fog nodes are usually used for the enlargement of the incited delay in the cloud environment. With regards to Blockchain and AI, these nodes will have to be enabled with Blockchain interface as well as outfitted with ML and AI capabilities, also the fog nodes perform the control and access of the data.

### B. Smart Contract

It is quite difficult to make sure that the implementation of a smart contract is firm against attacks and bugs free. The information and the code on the network are needed to be safeguard as they are vulnerable to attacks. This issue of vulnerability occurs because of the poor programming studies in the language in which the smart contracts are written. It has now become a critical significance for vulnerabilities for testing smart contracts, also for the smart contract code's security state new

tools have been formed. Besides, the outcomes of smart contract execution cannot be probabilistic. For decentralized AI, this can profess a key challenge in which the decision-making algorithms based on ML and AI get executed, in which the outcome of smart contract execution is usually in deterministic.

### C. AI Specific Consensus Mechanism

The consensus protocols that already exist considers the Blockchain network by facilitating the different proof of work or stake or X protocols. For future researchers, there are so many research opportunities are available, to investigate if the consensus protocol could be structured deliberating various verifications like the quality of optimization, efficient search strategies, efficient learning models.

### D. Lack of Standards

Until now, the standards of Blockchain technology are still needed to be advanced. Many institutions like IEEE, ITU, NIST are working on this, and many more has put forth the standards for Blockchain integration, architecture, and interoperability. Although, worldwide institutional and governmental guidelines should amend rules and regulations for the dispute handling, upliftment, and deployment of Blockchain, in the contrast of public Blockchain transactions using cryptocurrencies and AI applications. This involves research aimed at devising models.

### E. Data Quality and Quantity

AI applications are very much reliable on the data which is being provided to them. So, the quality of the data plays a very important role in building the AI application accordingly. If the data is biased the application will also work in that way only. Secondly quantity of the data is also important. Huge amount of data is required by one single AI application to work perfectly. If data is not enough for the proper working of the application, then AI will not be able to analysis all the problems. Providing the best quality and quantity of data is difficult for the companies.

### F. Case Specific Learning

Artificial Intelligence lacks behind human intelligence in communicating things. The data which is stored and collected by AI while performing a task or solving a problem may be useful in some other technology. But extraction of that data from the AI machine and to use it in different technology is very difficult because AI is case specific language. Transfer of data will require a lot of time.

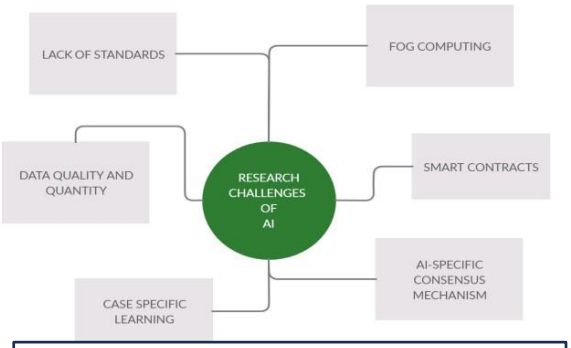



Figure 5. Challenges for Blockchain

## Conclusion

There is no denying the rapid pace at which blockchain- and AI-based concepts are being adopted. However, although both paradigms bring something new to the table, the level of originality and complexity varies widely. Because of the prevalence of digital currency in today's society, blockchain technology may one day automate payments and facilitate the secure, distributed transfer of sensitive data, information, and transaction records. Both blockchains and AI have been in the spotlight recently. Blockchain technology automates bitcoin payments and gives users access to a shared ledger of records, transactions, and data

using a decentralized, secure, and trustworthy system. A central authority may not be necessary for blockchain technology's smart contracts to govern user interactions. AI, on the other hand, gives machines reasoning and decision-making capabilities on par with humans. However, combining these two technologies might cause a dramatic change in the market. Both technologies are state-of-the-art, but by combining them, work might be completed more quickly and with less effort. This realization led to the investigation of a rigorous assessment of blockchain and AI combination publications written between 2010 and 2023. This presentation examined the current state of blockchain and AI combinations, their applications, and the possible revolutionary effects of their unique traits. There were 121 distinct publications on this topic that were considered for this assessment in total. The belief in the potential of AI and blockchains is gaining more and more acceptance. The benefits of combining AI with blockchain technology are covered in this essay. The bulk of this analysis is devoted to the use cases for integration, including supply chains, financial services, healthcare, life sciences, smart grids, agriculture, and the IoV. Before concluding, issues including privacy and security, credible oracles, the security of smart contracts, and the consequences of their deterministic execution, scalability, and collaboration between off-chain and on chain data storage were covered.

**References**:

1. Manish Verma, 373862192 'Blockchain and AI Convergence a New Era of Possibilities'.

2. Prerna Gulati, Aditi Sharma, Kartikey Bhasin, Chandrashekhar Azad, 'Approaches of Blockchain with AI: Challenges & Future Direction '.

3. Hamed Taherdoost 'Blockchain Technology and Artificial Intelligence Together: A Critical Review on Applications'.

4. S. Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system' Tech. Rep., 2008.

5. Satarupa Saha, Bappaditya Jana, Jayanta Poray, 'A Study on Blockchain Technology' October 15, 2019.