Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

A thorough Analysis of Blockchain's Potential for Internet of Things Applications in Precision Agricultural Networks

Luxmi Sapra[1], Ankit Mathani[2], Gunjan Bhatnagar[3]

[1]Associate Professor, Computer Science & Engineering, School of Computer Science & Engineering, Dev Bhoomi Uttarakhand University, Chakrata Road, Manduwala, Naugaon, Uttarakhand 248007

[2, 3]Assistant Professor, Computer Science & Engineering, School of Computer Science & Engineering, Dev Bhoomi Uttarakhand University, Chakrata Road, Manduwala, Naugaon, Uttarakhand 248007

[1]socse.luxmisapra@dbuu.ac.in, [2]socse.ankit@dbuu.ac.in, [3]socse.gunjan@dbuu.ac.in

Article Info
Page Number: 4141-4159
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 25 March 2022
Revised: 30 April 2022
Accepted: 15 June 2022
Publication: 19 August 2022

Abstract

The Internet of Things (IoT) has been more well-known in recent years as a result of the many services it provides and the extensive ways in which it is used in the area of science and technology. Some examples include smart agriculture and smart home gadgets. We currently live in a world that is filled with technologically advanced devices, and we make virtually constant use of them. Because of the growing number of users and the rising volume of data that is being shared, a significant quantity of sensitive information is now at risk of being compromised. Therefore, it is necessary to make certain that the channels through which data is being transferred should reach securely to the endpoint without compromising the data's integrity, confidentiality, or authentication, and that the data that reaches its destination should not be altered or tampered with in any way. In recent years, a significant new method known as blockchain has been established. This method has the potential to contribute to improvements in areas such security and trust, speed, visibility, immutability, and traceability. Because of these facts, the purpose of this study is to investigate the capabilities of the blockchain as well as the effectiveness of using it to address the rising concerns about the performance and security of IoT devices related with precision agriculture.

Keywords
Internet of Things (IoT), Blockchain, Cryptography, GUID, and Security are some of the Keywords that may be found in this article (Global Unique identifier). PKI (Public Key Infrastructure) and Internet of Things difficulties

1 Introduction

We live in a world that is completely saturated with technological apparatus and equipment. The Internet of things is one of the most ground-breaking technological advances of the 20th century (IoT). Internet of Things (IoT) is a topic of ongoing study that is also playing an essential part in the development of the technology industry. The term "Internet of Things" refers to a new technological paradigm that is conceptualized as a worldwide network of

machines and gadgets that are capable of talking with one another [1]. It is also a smart network that links everything to the internet for the purpose of sharing data and interacting through information detecting devices such as sensors, gateways, etc. [1] It is also important to note that the Internet of Things is a network that connects everything to the internet. These devices have a limited capacity for power and storage and are severely lacking in resource availability [2]. Ashton first used the phrase "Internet of Things" in 1998, and ever since that time, substantial advancements have been made in the field of "Internet of Things" [3]. The number of smart devices that are linked to the internet is growing at a steady rate each year; if the rate of development continues at its current pace, the number of connected devices will reach 23.5 billion by the year 2029 [4]. The Internet of Things has a wide variety of uses in the fields of science and technology. Use cases include things like smart industrial, clever logistics, smart agriculture, intelligent transportation, smart grid[5,] smart environmental protection, smart safety, smart medical, smart wearables, and home gadgets. [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [7].

In light of the implementation of a great number of strategies for securing IoT devices, there will continuously be the emergence of new kinds of assaults brought about by variations in security standards. Even while IoT devices are safe on their own, as soon as they are connected to an unsecured network, they become susceptible to a wide range of dangers, including device authentication, DoS/DDoS attacks[8,] intrusion detection malware detection[9], and detection of malware [10,11]. Studies have shown that over seventy percent of smart gadgets are susceptible to cyberattacks. In addition, in the past, cybercriminals have used Internet of Things devices to launch attacks such as Mirai (2016), Persirai (2017), and BrikerBot (2017).

security[10]. In today's world, a great number of devices contact with one another on a regular basis, which results in the transmission of a significant quantity of data. The operations of surveillance and warfare make use of a significant number of important IoT systems, such as the Internet of Drones (IoD) and the Internet of Robotic Things (IoRT) [11]. Because of this, there is a significant risk of a breach in both the data's security and its privacy while it is being transferred, which is a big cause for worry.

In this context, Blockchain has swiftly established itself as a significant technological advancement in recent years. It is generally agreed that Satoshi Nakamoto was the first person to create a blockchain. Additionally, he was responsible for the introduction of the electronic cash currency known as "Bitcoin," which increased interest in the study of Blockchain [12]. The blockchain is a public, trustworthy, shared, and unchangeable record of all transactions. It also has decentralized storage, provides high levels of transparency and security, and has these features [10]. Transactions are used to create blocks, which are then linked together in a chain using the information contained in neighboring blocks through a process known as hashing. Using a number of different cryptographic algorithms, these records have been safeguarded from being altered or tampered with [12]. Since its conception, blockchain technology has been connected into a number of different domains to manage a wide range of issues and bring improved answers to already existing ones. One of these areas is the Internet of Things (IoT). Blockchain technology has the potential to

address concerns about privacy, security, and a general lack of trust in the context of the Internet of Things. As a result, the use of Blockchain technology in the IoT sector has resulted in the birth of a new Blockchain sector in the IoT sector known as blockchain internet of things (BIoT) [13].

The following description illustrates how the document is structured. The introduction may be found in the first section. The second section covers the connected work. Blockchain technology and its specifications are covered in Section 3. The difficulties associated with securing IoT devices for precision agriculture are discussed in section 4. In the last segment, section 5, the Internet of Things performance problems are presented.

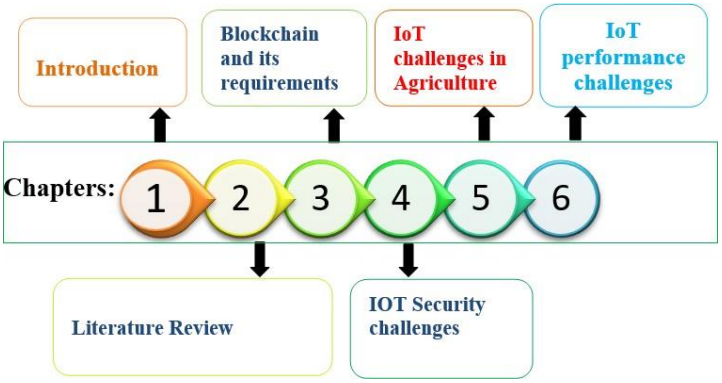

Fig. 1. A graphical layout of manuscript

1 Literature Review

A hybrid security approach in healthcare services was developed by M. Elhoseny and colleagues [14] to protect the diagnostic text data included in medical pictures while they are being sent. After developing the model utilizing a method known as 2D Discrete Wavelet Transformation 1 Level (2D-DWT-1L) steganography, we merged it with a hybrid encryption scheme that includes of both AES and RSA algorithms. This allowed us to conceal the fact that the model had been generated. The model was used on both the DME datasets and the DICOM datasets. Both sets of data were analyzed. The findings showed that the model has a PSNR value of 57.02 and an MSE value of 0.1288, both of which indicate that it performs better than the one that is currently in use. In a separate piece of research, Khari et al.[15] examined the use of cryptography and steganography in order to ensure the safety of data stored in Internet of Things (IoT) devices during transmission. The EGC protocol used cryptography in order to encrypt data, and steganography was used in order to conceal the encrypted data within low-complexity images. The work described in this paper focuses on the security of data stored in IoT devices. When compared to the methods that are already in use, the efficiency of the work that was presented (EGC) was 86%. S.Aggarwal et al.[29] proposed a model for the internet of drones that offers secure communication, data collection, and transmission among drones and users as well. This was accomplished through the utilization of a public blockchain that was built on the Ethereum platform, which included the selection of a forger node, the creation of blocks and validation, and the application of a proof-of-stake mechanism. It was determined based on the findings that the

This made the system more scalable, reliable, and superior by analyzing the computing cost and time. The suggested model addressed all security features such as AAA (authentication, authorization, and accountability), DI (data integrity), IA (identity anonymity), and VV (verification and validation). In a separate piece of work, M. Nikooghadam and colleagues [17] developed a secure and lightweight authentication and key management protocol for Internet of Things-based wireless sensor networks in order to establish a secure communication channel between user and sensor nodes. The instrument known as Automated Validation of Internet Security Protocol and Applications (AVISPa) is the mechanism that is used for forward verification. When compared to the protocols that are currently in use, the findings of the study demonstrated that both the transmission cost and the storage cost exhibited significantly improved performance.

SASH is the name of a framework that was presented by HTT Truong and colleagues [18], and it merges blockchain technology with the Internet of Things platform. This offers a multitude of benefits, including data transfer and security among IoT devices. Essentially, blockchain technology is used in SASH, and this technology includes a data marketplace, two different sharing methods, and prefix encryption. Firmware and Hyperledger have been used in order to develop SASH as a platform. The suggested job indicated a reasonable amount of administrative burden. In a separate piece of research, Karati et al. [19] suggested a novel generalized CLSC (gCLSC) Cryptography, certificateless signcryption approach to guarantee the safe transmission of data over IoT devices. It serves both as a digital signature and as an encryption method, and it may be used in situations in which authenticity, secrecy, and a minimal amount of overhead are important features. The performance meter of the suggested study showed that the computational cost was significantly improved, and moreover, the gCLSC observed minimum storge that was about fifty percent lower when compared to the CLSC.

A. Seyfollahi and colleagues[20] have suggested an algorithm known as Harris Hawks Optimization as a method for the reliable transmission of data for the internet of things. In order to guarantee accuracy and safety throughout the data aggregation process, the mechanism is designed using a fuzzy hierarchical network architecture that is compatible with Wireless Sensor Networks (WSN). When compared to other approaches, the findings demonstrated that RDD significantly improved the energy consumption, packet forwarding distance, and packet delivery ratio. Specifically, these metrics increased by 3.12%, 17.5%, and 43.5%, respectively. SP Gochhayat et al. [21] introduced a new distributed key management strategy for Internet of Things devices. This approach protects user sensitive data while still maintaining the user's privacy. This entity then collaborates with other peer entities to create an authentication mechanism. The technique involves outsourcing the resource-consuming cryptographic work to a local entity. The method also makes use of mobile agents by deploying them in subnetworks as necessary in order to take use of their many benefits. The findings of the study report showed that it had a beneficial effect on the reduction of the communication overhead.

A node-oriented secure data transmission (NOSDT) technique was created by X li et al. [22] for the purpose of protecting the transmission in social networks that are based on IoT. This

was done because nodes are very susceptible to assaults by other malicious nodes. The technique examines the actions of the malicious node and then selects replacement nodes that are dependable in order to ensure the security of data transfer. The transmission in malevolent nodes is intended to be decreased via the influence model. After being evaluated, NOSDT was shown to increase the performance of social networks by minimizing the influence that malicious nodes had on transmission. In a separate piece of research, MA Khan and colleagues [23] presented a blockchain-based solution for safe and confidential Internet of Things (IoT) communication inside a smart home network. Deep Extreme Learning Machine is used to enhance the capabilities of blockchain-based smart home architecture. Extreme Learning Machine, often known as DELM, is a feedforward neural network. It learns very rapidly. During the learning phase of this suggested system, the backpropagation technique was applied, and the network made adjustments to its weight in order to obtain accuracy. The accuracy of the suggested method was 93.91 percent, which was better than the performance of existing algorithms.

Super ChaCha is an improved version of the regular ChaCha stream cipher technique that was presented by MS Mahdi et al. [24] for the purpose of protecting data flow in IoT devices. In order to make a modification to the method, a change is made to the rotation. The input cipher went through many iterations, including column, diagonal, zigzag, and variant form. According to the findings, Super ChaCha was able to pass all five benchmarking tests and the NIST test with flying colors. Despite just a marginal rise in the amount of time, memory, and power required, as well as a marginal reduction in throughput, the complexity level was significantly increased. In order to crack Super ChaCha using a brute-force assault, you need need 2512 probable keys. Also, BM Pampapathi et al. [25] offered an efficient and reliable data distribution as well as a secure data transfer utilizing IANFIS (enhanced adaptive neuro fuzzy inference system) and MECC (modified elliptical curve cryptography) in the Internet of Things. Methods such as registration and data transfer, sending, data brokering, security analysis, and local computations are included in the work that is being suggested. When compared to ANFIS and IANFIS, the performance of IANIFS was found to be superior. In contrast, the MECC shown a 96% improvement in terms of its security in comparison to the present ECC.

In their study on the industrial Internet of Things, Manogaran et al. [26] suggested a paradigm for blockchain-assisted safe data sharing (BSDS). The objective is to get a maximum reaction rate while simultaneously minimizing FAP (false alarm progression). This model is responsible for ensuring the safety of data gathering and dissemination on both the incoming and outgoing sides. It was discovered that the BSDS was able to obtain a high response rate of 5.67% with a FAP of 4%, and it was also able to lower the failure rate by 2.14% with a FAP of 2%, respectively. In addition, it minimized the FAP by 3.12% while maintaining a response rate of 0.95, maximized the response rate by 6.63% while maintaining a failure rate of 0.06, and minimized the delay by 11.91% while maintaining a FAP of 5.2%. An identity-based online/off-line signcryption (OOSC) approach has been suggested by V.S. Naresh et al. [27] in a separate body of work. This technique is ideal to offer secure message transmission between IoT devices, gateways, and servers. This strategy

may be broken down into two distinct phases: online and offline. The offline phase is responsible for completing intensive mathematical calculations, while the online phase is responsible for performing less intensive computations. The results of the experiments showed that the suggested approach requires less time for calculation and offers protection against IND-CC2.

A system for the Internet of Things (IoT) called FL2S, which is based on federated learning and safe data sharing, was suggested by Q. Miao et al. [28]. FL2S was designed to ensure that data is shared securely. A framework known as federated learning (FL) is created based on the sensitive task decomposition. In addition, the technique known as deep reinforcement learning (DRL) is used in order to enhance the quality of data exchange. According to the findings, FL2S provided superior protection of user privacy and maintained higher data quality throughout safe data transfer. The numerous methods of safeguarding data that are used in IoT devices are broken down into their respective outcomes and problems and shown in Table 1.

Table 1. Represents the various security techniques utilized for securing data communication indifferent IoT domains

Author	Year	Technique/ Method	Result/challenges	Domain
M.elhoseny et al.[14]	2018	(2D-DWT-1L) Steganography integrated with AES and RSA.	Better performance in hiding confidential data into transmitted cover image and securing.	Healthcare based IoT.
Khari et al.[15]	2019	Elliptic Galois cryptography.	EGC showed 86 % better efficiency.	IoT.
S. Aggarwal et al.[29]	2019	Public blockchain on Ethereum platform.	Better computational costand time. It can also be performed onprivate blockchain.	IoD (internet ofdrones).
M. Nikooghadam et al. [17]	2019	Authentication and key management protocol (AVISPa) tool.	Better communication andstorage cost. No machine-to-machine security protocol in industrial IoT.	IoT
HTT Truong et al.[18]	2019	SASH, integrating blockchain with IoT platform.	Showed moderate overhead. SASH is yet to be implemented in global policies in network.	IoT.

A. Karati et al.[19]	2019	gCLSC Cryptography, certificateless Signcryption.	Minimal storage i.e. 50% less on comparing CLSC. Can be enhanced by incorporating revocation and discarding the bilinear pairing efficiently.	IoT.
A. Seyfollahi et al. [20]	2020	Reliable Data Dissemination for the Internet of Things (RDDI) Using Harris Hawks Optimization	Improved energy consumption, packet forwarding distance, and packet delivery ratio by 3.12%, 17.5% and 43.5 %	IoT.
		(HHO).	respectively. Yet to be evaluated on jamming attack.	
SP Gochhayat etal. [21]	2020	Delegating the resource consuming cryptographic to local entity.	Reduced the communication overhead, generation of extra certificates.	IoT.
X li et al. [22]	2020	Node oriented secure data transmission (NOSDT).	Improved performance of social networks by reducing the transmission impact of malicious nodes. More work can be done on forwarding path, better methods for detection of malicious nodes.	Social network in IoT.
MA Khan et al.[23]	2020	Blockchain empowered with Deep Extreme learning approach (DELM).	Accuracy = 93.91%. Exploring extensions through the application of further datasets and architectures.	Smart home IoT.
MS Mahdi et al.[24]	2021	Super ChaCha.	Increased complexity time, requires 2512 keys to break brute force attack.	IoT.

BM Pampapathi et al. [25]	2021	IANFIS (improved Adaptive neuro fuzzy inference system) and MECC (modified elliptical curve cryptography).	Better performance than ANFIS, also MECC is 96% better when compared to ECC.	IoT.
Manogaran et al.[26]	2021	Blockchain assisted secure data sharing (BSDS).	5.67% high response rate with FAP of 4% and reduced the failure rate by 2.14% rate with FAP of 2%, respectively	Industrial IoT.
V. S. Naresh et al.[27]	2021	Identity based online/off- line signcryption scheme (OOSC).	Less computational time and secure against IND-CC2. Yet to be implemented in healthcare monitoring systems and in industrial systems.	IoT.
Miao et al.[28]	2021	Federated Learning based Secure data Sharing (FL2S).	Better privacy protection and data quality in securedata sharing.	IoT.

The above research makes it abundantly evident that a significant number of the methodologies deployed are predicated on cryptography, which presents a potential security risk for IoT networks. Therefore, it is abundantly evident that a reliable solution such as blockchain is required to address a number of the problems stated in section 4. The Prerequisites for Blockchain Technology

Blockchain may be thought of as both an expanding list of records and a decentralized, unchangeable, distributed ledger that is used to keep track of time-stamped transactions that take place across numerous computers in a peer-to-peer network. The blockchain stores data in "blocks," which are then cryptographically connected to one another. A cryptographic hash of the block that came before it is included in each new block. A blockchain is the collective name given to all of these blocks after they have been linked together to create a chain. A blockchain's consensus process is activated each time a new block is added to the ledger.

guarantees that there is one and only one version of the truth that is accepted by all of the nodes that make up the Blockchain [30]. Figure 1 presents a diagrammatic representation of blockchain technology.

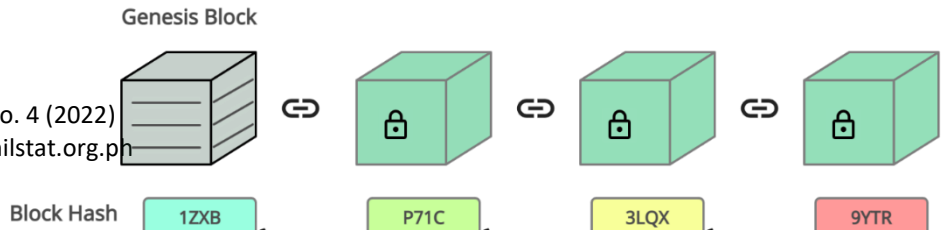

Fig.1. Blockchain consisting of blocks linked via hash codes[30]

Blockchain technology is made up of a few different components, all of which are necessary for the blockchain process to function properly. When creating new blocks, adding to existing ones, or saving data in blocks, there are protocols that must be observed. The following are some of the most important prerequisites for Blockchain:

- • Smart Contracts: A smart contract is a computer program that, when certain criteria are satisfied, is saved on a blockchain. This software makes a transaction both transparent and irreversible.
- • Tokenization permits the digital representation of rights, products, and services; it is used in blockchain technology. Users are able to communicate and build trust with one another via the usage of tokens, which eliminates the need for any centralized authority.
- • Data security: In order to prevent tampering with data, ensuring data security is an essential component of blockchain technology as well as an important part of this technology.
- • Distributed or dispersed computing environments need the use of decentralized data storage as a requirement.
- Immutability: In a distributed ledger, none of the records or transactions that have been saved should be changed in any way. This guarantees the confidentiality and safety of the data.
- •Consensus: This function ensures that new blocks are only added to the blockchain after receiving the unanimous approval of all legitimate users participating in the network.
- • Typed Blocks: This functionality is required for both high-speed commercial transactions as well as smart contracts. Therefore, the formatting of the various kinds of blocks, which includes the amount of time, the consensus technique, the number of transactions per block, and the data types of material it has, is distinct from one another.
- Sharding is essential because it allows the material to be distributed among a smaller group of nodes, hence reducing the workload on each individual node.

- Access rights management: A cryptographic technology, such as private and public key encryption cryptography, as well as distributed databases with user identities, are required for controlling access privileges and assigning a purpose. This may be accomplished via access rights management.
- • Standards that are used in the administration of permissioned blockchains: Only the data in a certain sequence may be seen since the blockchain network itself is immutable and cannot be changed in any way. Those who do not have access to the private key will not be given power, despite the fact that public certificates are viewable on the public blockchain. As a direct result of this, the data should consistently be structured in accordance with data features such as the user's IP address, name, code, and XML format. All of this information is sent across the consortium as an integral component of the communication process.
- • Application Programming Interfaces (API) must be taken into consideration when standardizing data formats. This is another need for blockchain-based systems. Any organization that participates in the blockchain network is required to employ similar data formats in order to interact inside the comparable network.
- Updatability: The ability to format and update data in a systematic way is required for every node in a peer-to-peer network that carries out a transaction. This is because updating the data in a distributed ledger is a crucial component for keeping records.
- • Encryption of peer-to-peer communications between blockchain nodes Blockchain technology necessitates the use of encryption to safeguard financial transactions among end nodes that may join forces.
- • User experience (UX): The user interface, also known as the user experience (UX), is one of the most significant parts of a system since it provides users with a straightforward and user-friendly application environment [30].
- Concern Regarding Safety in Internet of Things
- The security of IoT devices is very necessary for the efficient operation of the system. There are a number of different security considerations that need to be thought through. As a result, in order to make the IoT network safer and more dependable, we need to address the security concerns. The following is a list of some of the criteria that we need to concentrate on: [31]
- Maintaining confidentiality requires, at its core, concealing information from others who do not have permission to access it. The Internet of Things gathers a variety of private data from numerous sensors embedded in gadgets, such as those found in medical and healthcare equipment, as well as temperature, pressure, and heart rate monitors. It is possible to track down the essential particulars produced by these gadgets. Consequently, it is necessary for sensor devices to ensure the privacy of every piece of information they communicate.
- • Integrity may be described as the prevention of unauthorized persons in the

communication process from making changes to the data. In the internet of things, a single modification to a single data bit has the power to transform the whole meaning from "NO" to "YES."

- • Availability is something that can be described as the services that are operating the system being accessible at all moment to everyone who is an authorized entity. This should be the case at all times. Availability in a smart home should be able to execute at any moment in response to a request made by the user [32]. One example of this would be shutting off smart lighting using a remote control.

- • Trust and Privacy: Both trust and privacy are essential components of secure Internet of Things implementations. Trust management in the Internet of Things entails the trustworthy collection of data, the reliable fusion and mining of data, as well as the reliable enhancement of user privacy. Some of the factors that go into determining trust include the frequency of responses, the consistency of replies, physical closeness, shared goals and objectives, shared ecosystems, a history of involvement, and availability. The protection of one's privacy is another essential component. It is defined as the act of not disclosing any information about a person to any third party without first obtaining that person's permission. In the Internet of Things, data collecting is very important in public services; hence, the individual is the only one who can decide what information can be shared and with whom it should be shared.

- • Authentication and Access control: Authentication denotes a state in which both parties involved in a communication are certain that they are having a conversation with the real person to whom they are speaking. A reliable authentication system [33] will protect the data's privacy, maintain its integrity, and make it available without compromising its accessibility.

- • Accountability: In the setting of a heterogeneous Internet of Things, accountability assurance may be of assistance in determining which device created which data and also which device processed which data. It is the capacity to hold individuals responsible for the actions they do.

- • Auditability: This simply implies that in order to offer auditability for an Internet of Things system, we need to be able to monitor every event that takes place inside that system.

- • Non-repudiation: In the context of the Internet of Things, "the system must ensure whether the event happened or not" [34] is what is meant by non-repudiation.

- About the many concerns regarding the safety of IoT networks Blockchain has the potential to perform exceptionally well because to its centralized nature, immutability, traceability, fast speed, ability to store data, and ability to give security and privacy to users. As a result, it has the potential to perform better than the conventional procedures that are used. When working to improve the security of the internet of things, here are some crucial concepts to keep in mind. Blockchain technology has the potential to resolve a wide variety of problems. Blockchain technology also has the potential to

strengthen the previously stated security standards.

- 2 problems caused by the Internet of Things in precision agriculture: a case study
- Blockchain technologies have the potential to mitigate the risks associated with the Internet of Things (IoT) networks and, in tandem with this, give answers to some of the most significant problems facing precision agriculture, which are outlined below:
- • Expanding Address Space The limited address space available in the IPv6 communication protocol poses a substantial scaling challenge when it comes to the addressing of Internet of Things devices.
- devices. IPv6 only has 128 bits of address space, whereas blockchain has 160 bits of address space available to users. Taking into account a 160-bit address space, blockchain technology has the potential to generate and assign address spaces totaling around 1.461048 to IoT nodes. Because of this, the probability of an address collision is very remote. This is safe and more than enough to serve as a GUID for Internet of Things devices (Global Unique Identifier). Therefore, the use of blockchain technology does not need the need for a central authority to give and produce restricted Internet Assigned Number Authority.
- • Managing the Identities of Things: Blockchain technology may be used to generate identities that can be relied upon, as well as monitor ownership of goods, services, and products. Data transparency and traceability throughout the whole process are two additional benefits offered by blockchain technology. For example, there is a protocol called Trust-Chain that has been developed for authenticating and managing trustworthy transactions across dispersed Internet of Things networks while keeping the networks' integrity intact. Every single block that makes up the Trust-Chain indicates a transaction that took place between two participants in the IoT. Additionally, the hash codes of previous transactions are used in the production of new transactions. The primary advantage of Trust-Chain, in addition to its security features, is that each and every agent inside the system watches the interaction of others and accumulates information to determine trustworthy levels. In addition, blockchain technology has the potential to offer control mechanisms for transactions that are both trustworthy and decentralized. In addition to that, it offers speedy end-to-end data verification and remote asset management for Internet of Things devices.
- Verification of Transactions Conducted by the Internet of Things Blockchain networks have the potential to play a key part in the authentication and authorisation of Internet of Things (IoT) systems. Blockchain technology allows for whole Internet of Things transactions to be recorded on a distributed or shared ledger, which can then be monitored and tracked in a secure manner. Each and every Internet of Things transaction that is communicated with the blockchain system will always be cryptographically confirmed by the legitimate sender, who has a one-of-a-kind PK (Private Key) and GUID. As a direct consequence of this, confirming the authenticity and integrity of the triggered or activated transaction would be far less difficult.

Blockstack is a well-known blockchain solution that facilitates straightforward authentication of Internet of Things (IoT) transactions via the use of JSON Web Tokens (JWT). Blockstack's potential uses include the authentication of access in smart greenhouses, which is one of the applications for this technology.

- • Protecting Communications Within the Internet of Things Many traditional protocols, such as DTLS and TLS, have certain restrictions, especially when it comes to the amount of processing time or memory that is required. In addition, when employing the standard protocol for public key infrastructure (PKI), these solutions have some problems with centralized governance as well as control over the generation and distribution of keys. The blockchain has the potential to alleviate these problems and enhance key management among Internet of Things devices if it were to provide each and every device its own unique pair of GUID and PKI; once the blockchain was installed, it would be linked to the network. Additional secure communication improvements are conceivable with the assistance of blockchain technology. One example of this would be doing away with the need of a handshake phase in the DTLS or TLS protocols to exchange PKI certificates. As a consequence of this, blockchain would be the optimal option for addressing the requirements of runtime computing and memory management if the goal is to provide safe interactions between IoT devices. In addition, the firmware of Internet of Things devices may be hashed continually into a blockchain, which can then be used to detect IoT malware and notify device owners so they can take the appropriate precautions to protect their devices from the discovered dangerous bot. A message that is going to be sent to another IoT node is hashed by the transmitter node, and the hash code is then stored in a Blockchain network. On the other side, the message is hashed by the recipient node, which is an identical copy. According to the verification protocol, the message has not been altered or tampered with while it was being sent if the hash value on the message that was received is identical to the hash value that is stored on the Blockchain [35].

difficulties in achieving optimal performance with IoT and its blockchain-based solutions

- In the future, IoT systems will need to be able to coordinate a wide range of network topologies in order to accommodate the growing number of Internet of Things devices that are connected to precision agricultural networks.

- and analyse enormous volumes of data in a very short length of time. As a direct consequence of this, the functionality of IoT networks in precision agricultural systems presents some much more difficult issues. As seen in figure 2, there are five impediments that might be considered Internet of Things performance concerns in precision agricultural networks. Even with problems of this kind, the blockchain technology may be of assistance.

- Concerns Regarding Blockchain Technology and Sensing: This problem manifests itself in the IoT model's perception layer in the majority of cases. IoT nodes are able to send and receive data through the IoT cloud, and many agricultural devices, such as

tractors, irrigation machines, smart greenhouses, and farming devices, contain embedded sensors. These sensors continually generate data about the operating status of the device, and they allow IoT nodes to send and receive data. In this example, blockchain technology may be used to keep track of all M2M transactions in addition to defining the communication protocols that should be employed amongst these sensors. For instance, IOTA, a recently released upgrade to the blockchain technology, was developed in such a manner that it enables huge transactions to be carried out in IoT devices by using both IOTA and DAG. IOTA's use is that it has the potential to solve the scale problem that exists in precision agriculture.

- Blockchain and the Problem of Excessive Energy Consumption: Primarily, this problem is connected to the Network layer in the IoT layer paradigm. As a rule, Internet of Things gadgets are low-constraint, which means that it is anticipated that they will be low-power devices as the use of IoT devices in precision agriculture becomes more common. In order to practice precision agriculture, wireless equipment are required; yet, their energy consumption is much higher than that of their cable counterparts. However, due to the decentralized nature of Blockchain, it could be able to adopt specific solutions to the problem of high energy usage. There is the potential for blockchain technology, such as a private blockchain, to be used in order to keep the ratio of high computing power to high bandwidth connection for an IoT node intact. Since blockchain uses decentralized ledgers, it will be able to contribute to the maximization of electrification by assisting in the establishment of decentralized energy ledgers for the various components that make up a precision agriculture network. These components include, for example, the monitoring of a variety of sensors and batteries. Because of blockchain technology, we will also have the ability to monitor in real time the amount of energy that is being used by the sensors and gadgets that are part of the internet of things [36].

- The Blockchain and Networks Complexity Problem: Once again, this problem impacts the Network layer in the IoT layer paradigm. Complex communications in the IoT network system are a direct result of the many different heterogeneous network topologies that are used in precision agriculture. For agricultural equipment to work together effectively in precision agriculture, they need to be able to communicate with one another across a variety of platforms and infrastructures. It is not impossible to do so; but, doing so will be challenging, expensive, and time-consuming. Therefore, in order to solve these problems, blockchain technology may provide assistance in the process of data collecting and administration by using secure networks that are based on standards. There will be less complexity in IoT communications as a consequence of blockchain's ability to manage communications among IoT devices according to design principles, and there will be a decrease in the amount of time it takes for data to be sent within precision agricultural networks [35].

- Bandwidth and latency in blockchain technology The problem that arises when it comes to the performance of the Internet of Things is bandwidth and latency in device communication. In the Internet of Things, data flow originates outside of the data

center. As a consequence of this, it is imperative that communication be enabled as quickly as possible among the vast number of dispersed IoT devices. A substantial number of different Internet of Things devices need to have their software updated on a regular basis. In addition, device communication necessitates the use of a large number of different route alternatives in addition to many layers of packet inspection. If blockchain were used instead of the data center, these problems would be significantly reduced. The decentralization that blockchain provides will allow for the load to be distributed closer to the endpoints. As a direct consequence of this, Internet of Things connection will be developed with minimal latency while simultaneously having wasteful bandwidth. Because of the rapidly expanding size of blockchains, the need for significant amounts of processing power, storage space, and bandwidth has become vital. On the other hand, these limitations may be circumvented by using a private blockchain, which has the capacity to carry out more than one thousand transactions per second on Ethereum or Bitcoin.

- Due to the rapid growth of IoT-precision agriculture networks, massive volumes of data need to be kept and managed utilizing flexible archives. Blockchain technology presents a challenge in this regard because of its limited storage capacity. Traditional cloud-based storage solutions have a restricted capacity for manipulating large volumes of data belonging to a wide variety of Internet of Things devices. Therefore, the imposition of this limitation was necessitated by the needs of real-time data monitoring, high availability, scalability, and security, as well as low latency. IoT endpoints would be able to carry out more real-time data analysis and manipulation if Blockchain-based storage was used. This would be the answer to the problems that have been brought up about the limitations of cloud-based storage. Because data stored in a blockchain cannot be altered in any way, it is an excellent solution for ensuring the availability of data as well as its security. Additionally, illegal data sharing might be a problem in the cloud, but blockchain gives clients the ability to build access protocols without depending on a third party. [35]

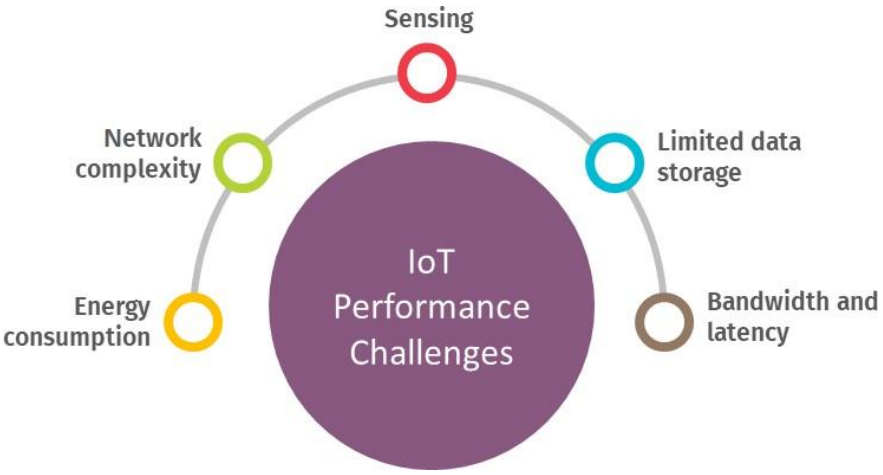

Figure 2. Five Obstacles to High-Performance Internet of Things

6 Conclusion

The Internet of Things (IoT) network is expanding at a breakneck pace in terms of both the breadth and depth of its penetration into various parts of society as well as its overall size. Because of the significant growth in use in modern times and the massive amounts of data that are being exchanged, data are now more susceptible to being compromised by malicious actors. Securing Internet of Things devices in order to make communication more secure and dependable is an urgent need in this day and age. The connection between Internet of Things devices may be made more secure with the use of blockchain technology. It is a distributed and immutable ledger that is both visible and traceable, and it offers a huge number of advantages. In this article, we took a high-level look at blockchain technology by conceptually describing it and analyzing its needs and specifications. There are a few advantages to using blockchain technology rather than more conventional approaches. A few topics pertaining to the Internet of Things were also brought up for discussion, including managing item identification, addressing address space, and transaction verification. It has also played an important part in providing solutions for IoT performance challenges in IoT precision agriculture, such as sensing, network complexity, energy consumption, limited data storage, bandwidth, and latency issues. These challenges have been addressed thanks to the work done by this technology. In addition to this, the foundation for a dependable precision agricultural infrastructure may be established. In the future, there will also be an application of a method that is based on blockchain technology to ensure the safety of the transmission of data in smart homes.

References

1. I. Lee and K. Lee, “The Internet of Things (IoT): Applications, investments, and challenges for enterprises,” Business Horizons, vol. 58, no. 4, pp. 431– 440, Jul. 2015, doi: 10.1016/j.bushor.2015.03.008.
2. U. Bodkhe and S. Tanwar, “Secure data dissemination techniques for IoT applications: Research challenges and opportunities,” in Software - Practice and Experience, Dec. 2021, vol. 51, no. 12, pp. 2469–2491. doi: 10.1002/spe.2811.
3. V. Bhuvaneswari and R. Porkodi, “The internet of things (IOT) applications and communication enabling technology standards: An overview,” in Proceedings - 2014 International Conference on Intelligent Computing Applications, ICICA 2014, Nov. 2014, pp. 324–329. doi: 10.1109/ICICA.2014.73.
4. “Estimated data on number of IoT devices connected worldwide.” https://www.statista.com/statistics/1183457/IoT-connected-devices- worldwide/ (accessed Jan. 17, 2022).
5. P. Anand, Y. Singh, A. Selwal, P. K. Singh, R. A. Felseghi, and M. S. Raboaca, “IoVT: Internet of vulnerable things? threat architecture, attack surfaces, and vulnerabilities in internet of things and its applications towards smart grids,” Energies (Basel), vol. 13, no. 18, Sep. 2020, doi: 10.3390/en13184813.
6. S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of IoT: Applications, challenges, and opportunities with China Perspective,” IEEE Internet of Things Journal, vol. 1, no. 4. Institute of Electrical and Electronics Engineers Inc., pp. 349–359, Aug.

01, 2014. doi: 10.1109/JIOT.2014.2337336.
7. "Real world examples of IoT." https://www.edureka.co/blog/iot-applications/ (accessed Jan. 17, 2022).
8. P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W. C. Hong, "Internet of things: Evolution, concerns and security challenges," Sensors, vol. 21, no. 5, pp. 1–35, Mar. 2021, doi: 10.3390/s21051809.
9. H. Wu, H. Han, X. Wang, and S. Sun, "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey," IEEE Access, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 153826–153848, 2020. doi: 10.1109/ACCESS.2020.3018170.
10. P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, "IoT vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges," IEEE Access, vol. 8, pp. 168825–168853, 2020, doi: 10.1109/ACCESS.2020.3022842.
11. Y. Shah and S. Sengupta, "A survey on Classification of Cyber-attacks on IoT and IIoT devices," in 2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2020, Oct. 2020, pp. 0406–0413. doi: 10.1109/UEMCON51285.2020.9298138.
12. M. Kamran, H. U. Khan, W. Nisar, M. Farooq, and S. U. Rehman, "Blockchain and Internet of Things: A bibliometric study," Computers and Electrical Engineering, vol. 81, Jan. 2020, doi: 10.1016/j.compeleceng.2019.106525.
13. B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, "Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions," Wireless Networks, vol. 27, no. 1, pp. 55– 90, Jan. 2021, doi: 10.1007/s11276-020-02445-6.
14. M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," IEEE Access, vol. 6, pp. 20596–20608, Mar. 2018, doi: 10.1109/ACCESS.2018.2817615.
15. M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 73–80, Jan. 2020, doi: 10.1109/TSMC.2019.2903785.
16. ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019.
17. A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," Future Generation Computer Systems, vol. 100, pp. 882–892, Nov. 2019, doi: 10.1016/j.future.2019.04.019.
18. H. T. T. Truong, M. Almeida, G. Karame, and C. Soriente, "Towards secure and decentralized sharing of IoT data," in Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019, Jul. 2019, pp. 176–183. doi: 10.1109/Blockchain.2019.00031.
19. A. Karati, C. I. Fan, and R. H. Hsu, "Provably Secure and Generalized Signcryption With Public Verifiability for Secure Data Transmission Between Resource-Constrained

IoT Devices," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10431–10440, Dec. 2019, doi: 10.1109/JIOT.2019.2939204.
20. A. Seyfollahi and A. Ghaffari, "Reliable data dissemination for the Internet of Things using Harris hawks optimization," Peer-to-Peer Networking and Applications, vol. 13, no. 6, pp. 1886–1902, Nov. 2020, doi: 10.1007/s12083- 020-00933-2.
21. S. P. Gochhayat et al., "Reliable and secure data transfer in IoT networks," Wireless Networks, vol. 26, no. 8, pp. 5689–5702, Nov. 2020, doi: 10.1007/s11276-019-02036-0.
22. X. Li and J. Wu, "Node-oriented secure data transmission algorithm based on iot system in social networks," IEEE Communications Letters, vol. 24, no. 12, pp. 2898–2902, Dec. 2020, doi: 10.1109/LCOMM.2020.3017889.
23. M. A. Khan et al., "A Machine Learning Approach for Blockchain-Based Smart Home Networks Security," IEEE Network, vol. 35, no. 3, pp. 223–229, May 2021, doi: 10.1109/MNET.011.2000514.
24. M. S. Mahdi, N. F. Hassan, and G. H. Abdul-Majeed, "An improved chacha algorithm for securing data on IoT devices," SN Applied Sciences, vol. 3, no. 4, Apr. 2021, doi: 10.1007/s42452-021-04425-7.
25. B. M. Pampapathi, M. Nageswara Guptha, and M. S. Hema, "Data distribution and secure data transmission using IANFIS and MECC in IoT," Journal of Ambient Intelligence and Humanized Computing, 2021, doi: 10.1007/s12652- 020-02792-4.
26. G. Manogaran, M. Alazab, P. M. Shakeel, and C. H. Hsu, "Blockchain Assisted Secure Data Sharing Model for Internet of Things Based Smart Industries," IEEE Transactions on Reliability, 2021, doi: 10.1109/TR.2020.3047833.
27. V. S. Naresh, S. Reddi, S. Kumari, V. V. L. Divakar Allavarpu, S. Kumar, and M. H. Yang, "Practical Identity Based Online/Off-Line Signcryption Scheme for Secure Communication in Internet of Things," IEEE Access, vol. 9, pp. 21267–21278, 2021, doi: 10.1109/ACCESS.2021.3055148.
28. Q. Miao, H. Lin, X. Wang, and M. M. Hassan, "Federated deep reinforcement learning based secure data sharing for Internet of Things," Computer Networks, vol. 197, Oct. 2021, doi: 10.1016/j.comnet.2021.108327.
29. ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019.
30. U. Bodkhe et al., "Blockchain for Industry 4.0: A comprehensive review," IEEE Access, vol. 8, pp. 79764–79800, 2020, doi: 10.1109/ACCESS.2020.2988579.
31. R. Malik, Y. Singh, Z. A. Sheikh, P. Anand, P. K. Singh, and T. C. Workneh, An Improved Deep Belief Network IDS on IoT-Based Network for Traffic Systems," Journal of Advanced Transportation, vol. 2022, pp. 1–17, Apr. 2022, doi: 10.1155/2022/7892130.
32. P. Anand, Y. Singh, A. Selwal, P. K. Singh, and K. Z. Ghafoor, "IVQFIoT: Intelligent vulnerability quantification framework for scoring internet of things vulnerabilities," Expert Systems, 2021, doi: 10.1111/exsy.12829.
33. P. Anand, Y. Singh, and A. Selwal, "Internet of Things (IoT): Vulnerabilities and Remediation Strategies."
34. C. Patel and N. Doshi, "Security Challenges in IoT Cyber World," 2019, pp. 171–191. doi: 10.1007/978-3-030-01560-2_8.
35. M. Torky and A. E. Hassanein, "Integrating blockchain and the internet of things in

precision agriculture: Analysis, opportunities, and challenges," Computers and Electronics in Agriculture, vol. 178. Elsevier B.V., Nov. 01, 2020. doi: 10.1016/j.compag.2020.105476.

36. K. Georgiou, S. Xavier-De-Souza, and K. Eder, "The IoT Energy Challenge: A Software Perspective," IEEE Embedded Systems Letters, vol. 10, no. 3. Institute of Electrical and Electronics Engineers Inc., pp. 53–56, Sep. 01, 2018. doi: 10.1109/LES.2017.2741419.