INTEGRATING IOT AND BLOCKCHAIN TECHNOLOGY FOR SECURING SENSORS COMMUNICATION

Sonali B. Wankhede[1], Dhiren Patel[2] and Mahesh Shirole[3]

[1, 3] VJTI, Mumbai, India
[2]SVNIT, Surat, India

ABSTRACT

Blockchain offers new approaches to manage and store data. The technical trajectory of blockchain makes it beneficial in various industries because of its benefits for tamperproof and immutable data security. The increasing use of IoT devices will surely result in a smarter world. A growing number of applications, including environment monitoring, building automation, smart metering, surveillance, and asset tracking, are turning to networks of wireless sensors, each of which is capable of a combination of processing, communication, and sensing. The Internet of Things (IoT) has facilitated the transition to a connected and intelligent digital environment, allowing smart manufacturing, improved decision-making and data analytics. In this study, we review the various IoT and Blockchain frameworks and discuss how integration of IoT and Blockchain resolves existing gaps.

KEYWORDS

Blockchain, IoT, IIoT, Sensors, Blockchain-IoT framework

1. INTRODUCTION

Technology advances have caused significant changes in our way of life over the past few decades, altering how we communicate, live, and work. The Internet of Things (IoT) is a collection of sensors, software, and other technologies that are used to gather and distribute data online. The potential of the convergence of IoT and Blockchain is fortifying security, enhancing privacy, and streamlining operations. Applications for IoT show the versatility and flexibility in a wide range of fields. The technology's capacity to improve traffic management, lower fuel consumption and enable autonomous cars has opened the path for intelligent transportation systems. IoT is also progressing significantly in fields like healthcare, transportation and urban planning.

Industrial IoT (IIoT) is transforming complicated industrial processes like manufacturing's predictive maintenance, resolving vulnerabilities for unauthorized access in Wireless Body Area Networks (WBANs) and implementing smart access control models. Numerous serious privacy, security, and management challenges have been brought on by the explosion in networked devices. These devices produce enormous amounts of data, which presents substantial issues for data management.

In addition to processing and storing this data, it also entails constantly preserving its reliability, validity, and accessibility. IoT devices are prone to cyberattacks by their very nature of

David C. Wyld et al. (Eds): SIPR, NCWC, BIBC, SOFEA, DSML, ARIA, NLP, CSEN -2023
pp. 85-95, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.131907

interconnectedness. It is necessary to address these issues by offering strong solutions, for protecting data, improving the privacy and guaranteed security.

Industrial Internet of Things (IIoT) has accelerated the growth of smart cities, improved resource management, affordable and on-demand manufacturing, renewable energy management and trading and other smart startup industries [6]. Several advancements in smart manufacturing units have garnered sporadic attention throughout the last 10 years. Industrial security systems, digital or connected factories, industrial configuration warnings, and maintenance safety make up the majority of the IIoT applications that are extensively utilized. Large technologies that will have a large influence on industry include blockchain and the Internet of Things [7].

Today, the Internet of Things, Cloud computing, Artificial intelligence, Drones, Mobile Apps, Smart Sensors and Blockchain are all used in smart farming and precision agriculture fostering efficient food supply chains [12]. It is now feasible to process and have access to real-time data regarding soil, crop, and weather conditions as well as other pertinent services like the supply chain for crops and fruits, food safety and animal grazing [12]. Combination of agricultural data, forecasting and predictive analytic software systems may give farmers advice on soil management [13], crop maturity rotation, the best times to grow and harvest their crops, and other topics. Additionally, IoT and sensor technologies can help precision agriculture overcome a number of obstacles. If straightforward authentication measures are not implemented on IoT applications or if access control mechanisms are poorly defined, cyberattacks may occur and put everything at risk [11]

Blockchain technology combines data exchange, processing, and storage technologies across numerous parties. We can leverage integration of IoT and Blockchain in a number of ways. Each data point is timestamped, hashed, and linked to the previous one. The decentralized nature of blockchain reduces the risk of a single point of failure. Access controls and encryption can further enhance data security.

The use smart contracts to automate actions based on IoT data triggers. For example, a smart contract could automatically execute a payment when a certain condition is met in the IoT data. Implementing blockchain in supply chains to track the origin and journey of products in real-time is valuable in industries like food and pharmaceuticals. Decentralized IoT networks can be created, where devices communicate directly with each other using blockchain as the trust and security layer, reducing reliance on central servers.

The rest of this article is organized as follows: Section 2 describes the Blockchain Technology and the major gaps that Blockchain can fix. Section 3 discusses the integration of IoT and Blockchain. Section 4 presents the framework to integrate IoT and Blockchain. Section 5 discusses the Blockchain and IoT Integration in Supply Chain Management. Section 6 concludes this paper.

2. BLOCKCHAIN TECHNOLOGY

Blockchain is a type of distributed ledger technology that enables the safe, transparent, and unalterable storage of data over many networks. The hash lock that connects each block in a blockchain to the one before it (using, for example, the SHA256 hash function) makes it nearly difficult to change data after it has been recorded. It is challenging for hackers or anybody else to infiltrate the system since data is kept over a network of computers instead of a single server. Transparency makes sure that every action is available for everyone to see and verify, which promotes cooperation and confidence. Data integrity is guaranteed by blockchain's immutability,

which precludes any tampering with the data that has already been recorded, particularly in circumstances when conventional data management solutions show to be insufficient or risky.

Blockchain has the potential to reduce costs associated with centralized energy delivery by enabling peer-to-peer energy transactions, improving overall energy efficiency. Essentially, Blockchains support smart contracts implementation. A computer program that can be executed is created from the accepted contract clauses. Every contract statement that is carried out results in an immutable transaction that is kept in the blockchain. Smart contracts ensure proper access control and contract enforcement [2].

Contract enforcement ensures that the contract execution is deterministic. Any time a smart contract's conditions are met, the triggered statement will predictably and automatically perform the relevant function. The rights, obligations, and limitations of contracts are first discussed and negotiated by a number of concerned parties. An agreement may be reached after several rounds of deliberations and negotiations [2]. Then, using computer languages like declarative language and logic-based rule language, software engineers transform this agreement written in normal languages into a smart contract. The deployed certified smart contracts can then be used on platforms built on top of blockchains. Because blockchains are immutable, contracts stored there cannot be changed. Consequently, a transaction is carried out and verified by miners in the blockchains. All parties involved are updated with new states following the execution of a smart contract. As a result, blockchains are used to store both the transactions that occur during the execution of smart contracts and the changed states.

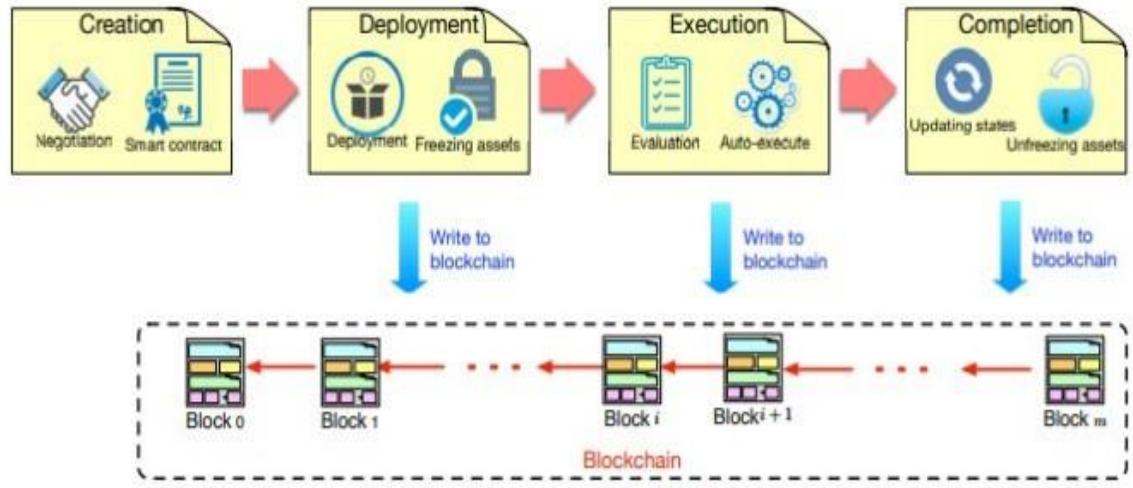

Figure 1. Life cycle of a smart contract [3]

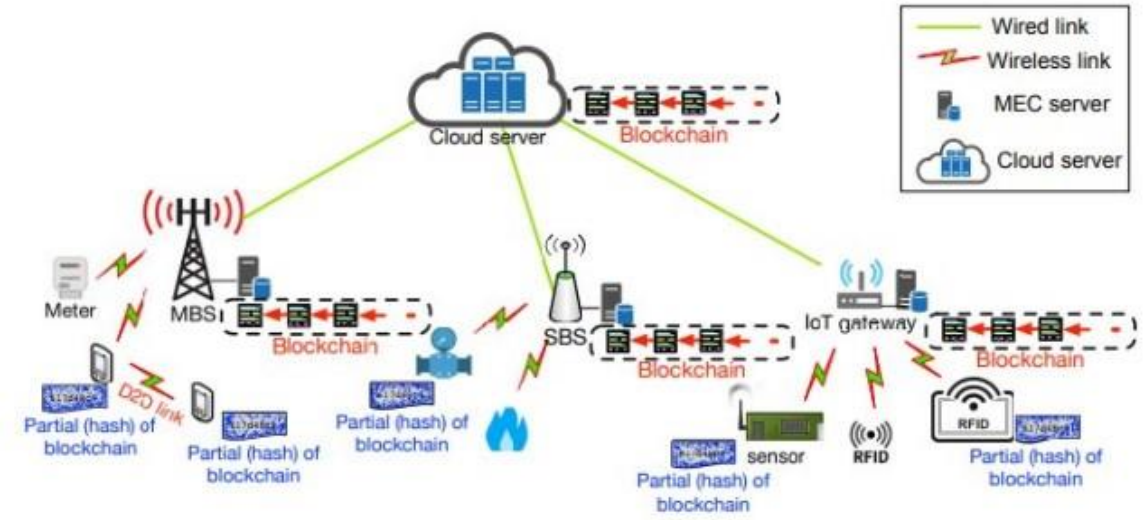

Figure 2. Deployment example of BcoT [2]

Some of the advantages of using Blockchain are as follows:

i. **Decentralization of data**: IoT data is frequently controlled and maintained by centralized servers, opening the door for other parties to hack into the private information. Additionally, the network can collapse right away. As a result of the blockchain's decentralized structure, which takes into account the absence of a centralized data storage and control point, there are no single sources of vulnerability. Despite clouds, the blockchain network is run by several separate locations, thus there is no one entity in charge of the vast majority of the data produced by IoT devices.

ii. **Update secure dives**: Since they can safely transmit the code on the IoT devices, developers are now able to address difficulties with out-of-date IoT software thanks to blockchain's greater safety and security procedures.

iii. **Improved privacy**: Even the connection between the devices may be concealed (pseudo-anonymously) via the blockchain, which also provides transaction confirmation. Additionally, the blockchain can provide the encryption and enhance the IoT protocols. As a result, there are less chances of data leaks and IoT network hacks.

iv. **Improved data administration**: IoT networks are expected to convey massive volumes of data in real time over many platforms, systems, and devices, creating new issues for data management. The blockchain (through Distributed Ledger Technology) enables direct and trustworthy data movement between devices without the need of a server, cloud, or local database. This reduces the number of transactions by at least one third. Additionally, smart contracts can automate the majority of interactions between IoT devices.

v. **Improved scaling**: The load is distributed among decentralized blockchain networks, resulting in better transaction processing (with high trust) and better coordination between the billions of IoT devices that are linked to them. Scalability is further aided by the ability of data to be shared.

3. IOT AND BLOCKCHAIN INTEGRATION

The IoT has demonstrated its ability to automate monitoring and operation in the home, workplace, and industry. However, for data processing, network command, and control, it depends on centralized cloud computing. Because IoT owners must rely on a third party (such as cloud providers) for the integrity of the data and the process outputs, the integrity of the data and the output of cloud computing is constantly in doubt with the centralized model [1]. On the other hand, a blockchain network's fundamental characteristics include trustworthiness, data redundancy, transparency, and verifiability. The gaps in delivering the security-related guarantees needed by an IoT network and related applications can be filled by these key aspects. The fundamental needs for massive storage, business/industry automation, fault-tolerance, and data integrity may thus be met by integrating an IoT with a blockchain network [1].

Supply chain management becomes a significant concern as the demand for effective logistics rises and global trade keeps expanding. Blockchain can provide seamless authentication, data privacy, security, resilience to attacks, ease of implementation, and self-maintenance. These two disruptive technologies coming together could spur technological advancement and innovation, helping to determine the future of the digital world. In a blockchain network, devices in an IoT network may be configured to perform a variety of functions. It is possible to create edge devices to store the blockchain and carry out transaction validations, including routers, routing switches, integrated access devices, multiplexers and gateways. To perform services for issuing transactions to a Blockchain Network (BCN) on behalf of the associated resource constraint devices, such as sensors, intermediate devices like relay routers can be developed [1].

4. IOT AND BLOCKCHAIN FRAMEWORK

- **IoT to IoT**: Since it just calls for the use of a shared register for IoT data storage, this is essentially the simplest method of integrating blockchain into the IoT network. The data will be sent outside of the blockchain utilizing a variety of routing techniques. As a result, there will be less delays and faster transaction speeds. This method also gives the devices the option of working offline. The only thing you need to do to set up the transmitting, storing, and extracting of data from blockchain rather than a cloud or a server is set up, making this a simple option to deploy as it does not need substantial modifications to the workflow of the IoT devices [4].

As shown in Figure 2, the physical layer, repository layer and application service layer are the three layers that make up the suggested system. The physical layer consists of sensors, actuators, and any embedded Internet of Things device like an Arduino or Raspberry Pi. Sensors are used to pick up events from the environment, such as the BME280 sensor, which measures pressure, humidity, and temperature. On the basis of a signal or a command, actuators are employed to control a device. To control equipment like a light, fan, motor, etc., actuators are employed. The physical layer and repository layer communicate using the MQTT protocol. In the physical layer, IoT devices have the ability to publish and subscribe to messages.

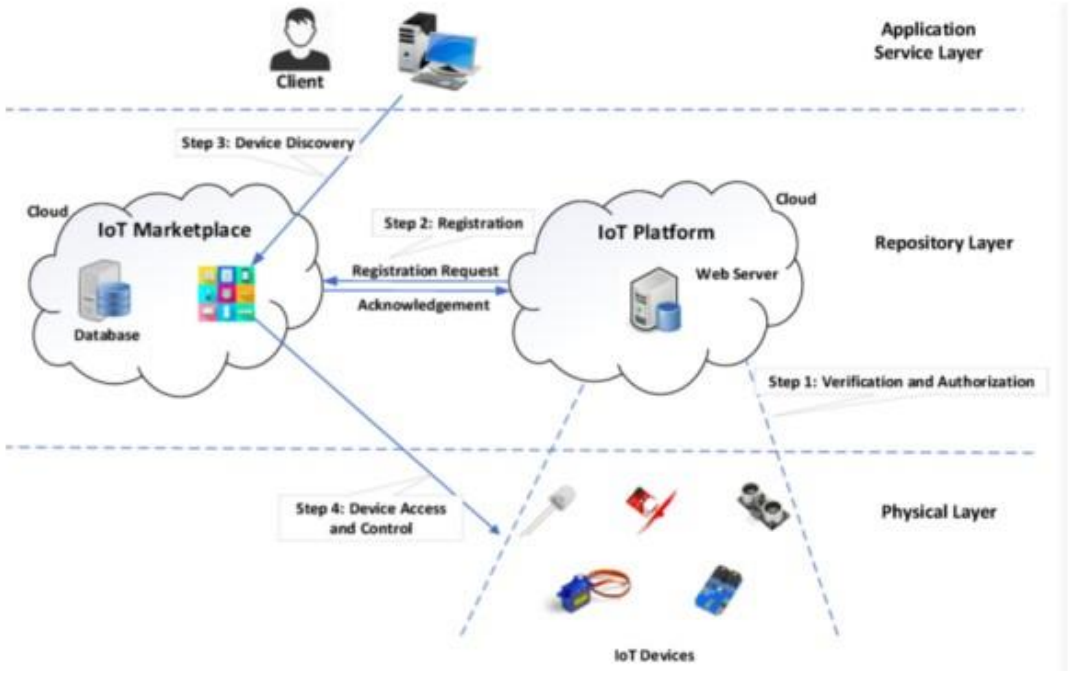

Figure 3. IoT to IoT Framework [9]

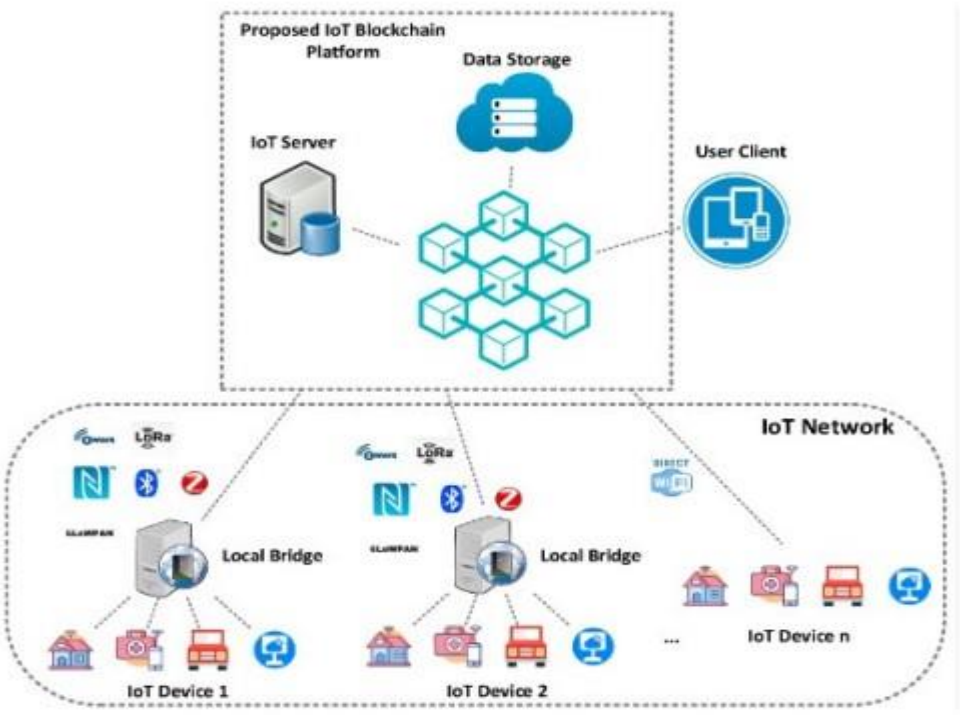

Figure 4. IoT and BLOCKCHAIN Framework [5]

- **IoT to blockchain**: In this method, IoT devices communicate with each other via the blockchain, which functions as a cloud for conventional IoT networks [4]. According to one perspective, this will improve tracing, communication security, workflow

automation, and capacity. If the blockchain is not quick enough, on the other hand, it will complicate the system significantly, which will lead to delays. The integration of this blockchain into IoT networks is challenging because it necessitates several adjustments to both the operation of IoT devices and blockchain development.

A suitable blockchain should be employed as well, one with greater operating speed, capacity, and no fees. This blockchain may be built on IOTA, Modum.io, or Riddle and Code. The IoT blockchain platform is conceptualized in Figure 4, which shows a vast array of IoT devices, data storages, user devices, servers, and local bridges connected by a peer-to-peer blockchain network. The services include gathering sensor data from the bridge, sending commands to control actuators, querying data and storing data via the blockchain network, among other things.

Profiles of physical devices, environmental data gathered by sensors, and profiles of device owners can all be stored in the blockchain network's data storage. Either a hard drive or a database can be used as the storage medium. Any terminal, including mobile phones, laptops, and desktop computers, can be a user client that allows people to read or publish data to the blockchain network. Local bridges function as both the service agent and the conduit between a group of IoT devices and the server.

- **Hybrid strategy**: In this scenario, the IoT devices share the majority of the data and interactions, with the blockchain merely storing specific sorts of data. This strategy introduces Fog Computing to overcome the limitations of blockchain and IoT devices. The complete architecture is shown in Figure 5, which includes two levels, blockchain and edge-based authentication layer. The central idea is to deploy a centralized authentication level to Internet of Things (IoT) devices that interface with network edges to process and store data [8].

  In order to provide decentralized authentication, a connection is then established between the edge networks and blockchain architecture. This connection allows the authenticated IoT devices and edge networks to communicate and share data in a secure manner [8]. The suggested paradigm enables secure scalability for heterogeneous IoT systems by enabling secure communication between IoT devices that are part of the same system or between devices from other systems. The edge server controls all requests made by IoT nodes, validates and authenticates them, and controls communication between the nodes [8].

  Each IoT system and its devices are connected to the closest edge server, and they are only permitted to communicate with other devices that edge server has registered and authorized [8]. The two major stages of centralized edge-level authentication are initialization and device authentication and intercommunication. To ensure that every node can be individually identified, the startup step enables the system and its linked smart devices to be registered on the edge network. The new system and the relevant gadgets join the network after being registered. Device authentication and communication inside the same edge network are part of the authentication and intercommunication phase. Edge servers are used to centrally authenticate devices.

  In Decentralized blockchain based authentication, the relevant edge servers register and certify the IoT devices. If the communicating devices are on the same edge server, the edge server stores the identity and credentials of the communicating devices, centralizing device authentication [8]. If the devices are part of groups on various edge servers, they are registered at the appropriate edges and are verified by the blockchain network.

When an IoT node transmits data, the relevant edge first verifies the transaction data before pooling it with other transactions. The edge node then creates a new block of transactions, which is signed and tied using a computed hash and nonce before being further verified by the mining process. The blockchain network then conducts a proof-of block validation to confirm the block's transactions. A block is regarded as having been added to the end of the blockchain if no errors are found.

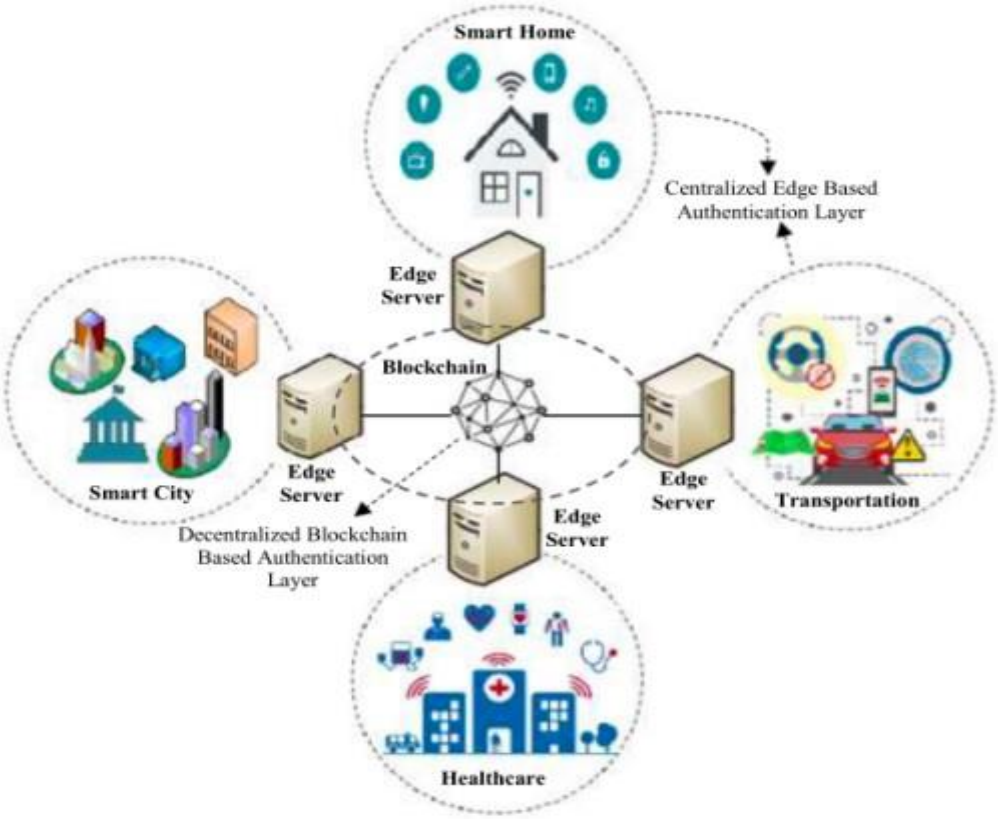

Figure 5. Hybrid blockchain-based architecture [8]

Table 1. Comparison of IoT and Blockchain Frameworks [10]

IoT to IoT	IoT to Blockchain	Hybrid Strategy
Direct data exchange takes place between IoT devices	Blockchain is used for interactions and communications	Edge computing is employed to establish a seamless environment for interaction
Needs complex routing and discovery procedures	The information can be recorded on blockchain	It uses Artificial Intelligence, fog computing and edge computing to build a seamless environment for IoT device interaction
It operates best when devices are on the same network or under a single domain	It is beneficial for IoT devices from different domains	Fog computing layer act as nodes on the blockchain and handle all transactions
It is beneficial when low latency	It is used where high fidelity of	It reduces energy consumption

and great performance are required	the data is required	and some of the bandwidth and latency problems

4.1. Advantages af Blockchain and Iot Framework

The solution to IoT privacy and dependability issues lies in blockchain technology. The IoT sector needs a silver bullet, and that bullet is blockchain technology. It may be used to monitor billions of linked devices, processing transactions and enabling device synchronization. As a result, the makers of the IoT business may save a lot of money. Single points of failure would be eliminated by this decentralized strategy, strengthening the device ecosystem. Blockchain's encryption algorithms would increase the confidentiality of customer data. The blockchain's key benefits include high levels of openness, greater security, improved traceability, high levels of efficiency, cheap costs, and the absence of third-party intermediaries. The catalysts to providing alternatives in consumer data management will be the mix of IoT enabled blockchain and well-designed incentives.

IoT systems need to have security built in from the ground up, with strict authority checks, authentication, data verification, and encryption of all data. With stronger code development standards, training, threat analysis, and testing, software development companies need to be better at building framework that is stable, robust, and trustworthy at the application level.

An IoT that protects privacy must be safe and secure. The key is to adhere to best practices while designing and implementing blockchain-IoT applications. Some of the practices are as follows:

1. Integrate and secure data to minimize cost and complexity while protecting organization investment.
2. Collect and manage data to build a platform that is standards-based, scalable, and secure.
3. Analyze data and take action by separating data's business value and doing something with it.

5. BLOCKCHAIN AND IOT INTEGRATION IN SUPPLY CHAIN MANAGEMENT

Blockchain and IoT integration in Food supply offers the potential to optimize supply chain processes by improving traceability, reducing operational costs, and enhancing overall supply chain security. They can also be used to elevate the efficiency, reliability, and transparency of supply chain management.

By eliminating the dependency on third-parties, integrating blockchain into the IoT framework enables the creation of a secure decentralized architecture, supporting the development of new business models. IoT system's dependability and scalability can be improved by using blockchain technology, especially smart contracts, to build trust for data and executed activities. A blockchain-based access control system that uses the ripple protocol consensus algorithm to include transactions into the blockchain can enable secure communication between drones and the ground station server in the context of the Internet of Drones (IoD).

In order to increase access control security in IoT, a methodology that uses zero-knowledge proof and smart contract technology within the blockchain is used to preserve data collected by the drones and make it tamper-resistant. According to the findings, deploying access control attribute data in a blockchain, using encrypted access control tokens, and implementing smart contracts all significantly improve attribute privacy protection, access efficiency, and risk mitigation in the IoT ecosystem when compared to traditional centralized access control models.

Security and authentication in blockchain-based IoT networks examine how blockchain might improve security and trust inside IoT networks through secure access management, effective authentication, key agreement, and secure communication. Peer-to-peer (P2P) nodes are necessary for the consensus process in blockchain, despite the fact that it also provides enhanced security and other advantages. IoT ecosystems, on the other hand, are by nature made up of a lot of P2P nodes, yet they are heavily criticized for lacking security safeguards. The result of the union of these complementing groups, has thus emerged as a new research trend, "Blockchain of Things (BCoT)",

6. CONCLUSION

IoT networks can benefit from blockchain technology's increased security and efficiency, as well as its decentralization and usage of smart contracts. However, the adoption of this technology comes with a number of issues, including the limited resources, inadequate encryption, scalability issues and communication protocols that concentrate on both IoT devices and blockchain networks. In this paper, we investigate the integration of IoT and Blockchain technology. We also discuss the different types of IoT and Blockchain frameworks.

REFERENCES

[1] Naresh Adhikari and Mahalingam Ramkumar. "Iot and blockchain integration: Applications, opportunities, and challenges", Network, 3(1):115– 141, 2023.

[2] Hong-Ning Dai, Zibin Zheng, and Yan Zhang "Blockchain for internet of things: A survey", IEEE Internet of Things Journal, 6(5):8076–8094, 2019.

[3] Ruizhong Du, Caixia Ma, and Mingyue Li., "Privacy-preserving searchable encryption scheme based on public and private blockchains", Tsinghua Science and Technology, 28(1):13–26, 2022.

[4] Karim Ennasraoui, Youssef Baddi, Younes El Bouzekri El Idrissi, and El Mehdi Baa., "Security analysis in the internet of things: State of the art, challenges, and future research topics", Advanced Intelligent Systems for Sustainable Development (AI2SD'2018) Volume 5: Advanced Intelligent Systems for Computing Sciences, pages 745–752, 2019.

[5] Lei Hang and Do-Hyeun Kim, "Design and implementation of an integrated iot blockchain platform for sensing data integrity", Sensors 19(10):2228, 2019.

[6] Saddam Hussain, Syed Sajid Ullah, Ihsan Ali, Jiafeng Xie, and Venkata N. Inukollu, "Certificateless signature schemes in industrial internet of things: A comparative survey", Computer Communications, 181:116–131, 2022.

[7] Pls Jayalaxmi, Rahul Saha, Gulshan Kumar, Neeraj Kumar, and TaiHoon Kim, "A taxonomy of security issues in industrial internet-of-things: scoping review for existing solutions, future implications, and research challenges", IEEE Access, 9:25344–25359, 2021.

[8] Osama A. Khashan and Nour M. Khafajah., "Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous iot systems", Journal of King Saud University - Computer and Information Sciences, 35(2):726–739, 2023.

[9] Faisal Mehmood, Shabir Ahmad, and DoHyeun Kim, "Design and implementation of an interworking iot platform and marketplace in cloud of things", Sustainability, 11(21), 2019.

[10] Clement Nartey, Eric Tutu Tchao, James Dzisi Gadze, Eliel Keelson, Griffith Selorm Klogo, Benjamin Kommey, and Kwasi Diawuo, "On blockchain and iot integration platforms: current implementation challenges and future perspectives", Wireless Communications and Mobile Computing, 2021:1–25, 2021.

[11] Wei Ren, Xutao Wan, and Pengcheng Gan, "A double-blockchain solution for agricultural sampled data security in internet of things network", Future Generation Computer Systems, 117:453–461, 2021.

[12] Streche, Robert, et al. "IMPLEMENTING BLOCKCHAIN TECHNOLOGY IN IOT VINEYARD MONITORING SYSTEM", Air & Water Components of the Environment/Aerul si Apa Componente ale Mediului (2023).

[13] Mohamed Torky and Aboul Ella Hassanein, "Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges", Computers and Electronics in Agriculture, 178:105476, 2020.

AUTHORS

Sonali B. Wankhede received the B.E degree in Computer Engineering from Xavier Institute of Engineering, Mumbai, India and M.E degree in Computer Engineering from Thadomal Shahani Engineering College. She is currently pursuing PhD in Computer Engineering from VJTI, Mumbai, India. She has 9.7 years of experience as an Assistant Professor at various renowned institutes across India. Her research interests include Blockchain Technology, Cyber security, Internet of Things (IoT).

Dhiren Patel is currently a Professor of Computer Science & Engg at NIT Surat, Gujarat, India. He has served as Director of VJTI Mumbai (for 5 years during 2017-2022). His research interests include Blockchain and DLT, Cyber Security, Trust Management, and Technologies for Sustainable Development. He has played a key role in designing Nation-wide centralized engineering admission systems in India (AIEEE/CCB and JoSAA), and in National capacity building in the areas of Cyber Security and Blockchain Technology through MeitY (Govt. of India).

Mahesh Shirole is Currently the Head and Associate Professor of Computer Engineering at VJTI, Mumbai, India. He holds a doctoral degree in Computer Engineering from Indian Institute of Technology, Kharagpur (IITKGP). His research interests include software engineering, blockchain technology, machine learning, networking, security, and evolutionary optimization.