DOUBLE BLIND PEER REVIEWED JOURNAL IMPACT FACTOR :7.8 7654:34XX(ONLINE)
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY FINANCE INSIGHTS

Leveraging Digital Innovation for Strategic Treasury Management: Blockchain, and Real-Time Analytics for Optimizing Cash Flow and Liquidity in Global Corporation

Vol.2 No.2 2023

Kulasekhara Reddy Kotte

SLRI Solutions, INC.

kottekula@gmail.com

Sr SAP Fico Consultant

Received on: 12 Jan 2023

Revised on: 15 Feb 2023

Accepted and Published: March 2023

Abstract:

Originally created for cryptocurrencies, blockchain technology has matured into a flexible instrument with a wide range of uses outside of finance. The security of Internet of Things (IoT) networks is one of the most potential applications of blockchain technology. Because Internet of Things (IoT) is decentralized and scalable, it presents substantial security challenges. IoT is defined by linked objects interacting over the internet. This article investigates how decentralized protocols based on blockchain technology can safeguard Internet of Things networks, providing solutions for authorization, authentication, and data integrity. Future directions for this domain's research as well as problems and real-world applications are covered in this study.

Introduction:

1.1 Overview of Blockchain Technology

2008 saw the introduction of blockchain technology with Satoshi Nakamoto's launch of Bitcoin. Presenting a decentralized ledger system that could function without a

central authority, the idea was revolutionary. In essence, the blockchain is a distributed database that keeps track of an ever-expanding list of documents known as blocks that are connected and safeguarded by cryptographic techniques. Every block forms an immutable and transparent chain with a date and a link to the block before it.

Although blockchain technology first became well-known for its use in cryptocurrencies, there are a wide range of other possible uses for it outside of the financial industry. Blockchain is an appealing option for many industries, such as supply chain management, healthcare, and, more recently, the Internet of Things (IoT) [1], since it is decentralized, transparent, and safe.

1.2 Overview of IoT Networks

A network of physical items, or "things," that are implanted with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet is described by the Internet of Things (IoT) concept. These "things" could be anything from basic industrial machinery to sophisticated home appliances [2]. Numerous facets of daily life, including smart cities and houses, connected cars, and industrial automation, could be completely transformed by the Internet of Things.

But the quick proliferation of IoT devices has also brought forth a number of serious difficulties, chief among them being security. IoT networks are susceptible to a variety of security risks because of the vast quantity of devices and the heterogeneity of hardware and software they employ [3].

1.3 Synopsis of IoT Security Issues

IoT networks confront numerous security issues, many of which are caused by the large number of devices and decentralized structure of the networks. These difficulties consist of, but are not restricted to:

Data Breaches: Because IoT networks create so much data, they are an attractive target for cybercriminals. Unauthorized access to this information may result in serious privacy violations [4]. Malicious actors may use Internet of Things (IoT) devices to launch distributed denial-of-service (DDoS) attacks or obtain unauthorized access to the network [5].

Weak Authorization and Authentication: A lot of Internet of Things (IoT) devices have very basic security features, and they frequently don't have strong authorization and authentication systems. This vulnerability may allow devices [6] to be accessed and controlled by unauthorized parties.

Problems with Scalability: With the increasing number of IoT devices, traditional centralized security measures find it difficult to scale efficiently, which could result in bottlenecks and single points of failure [7].

1.4 Reasons to Use Blockchain in Internet of Things

Blockchain technology is a viable resolution to numerous security issues that IoT networks encounter. The distributed architecture of the Internet of Things and the decentralized nature of blockchain complement each other effectively, offering a foundation for safe data storage and communication. IoT network security can be improved by utilizing key blockchain features including immutability, transparency, and consensus-driven verification [8].

Blockchain, for instance, can be used to guarantee the accuracy of data produced by Internet of Things devices. The blockchain allows for the recording of every transaction and data entry, making it easily auditable and tamper-evident. Furthermore, security policies can be automatically enforced by blockchain-based smart contracts throughout the network, lowering the possibility of malicious or human error [9].

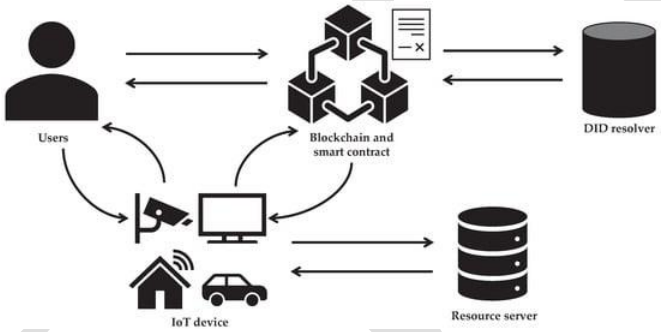

Fig 1: Decentralized IoT Access Control Architecture

2. Overview of Blockchain Technology

2.1 Foundations of Blockchain

Blockchain is a distributed ledger technology that enables decentralized data storage over a network of computers. A blockchain is made up of a series of blocks, each of which has a list of transactions, a timestamp, and a link to the block before it. Cryptographic hashing is used to protect this chain, making it immutable [10] because once data is recorded, it cannot be changed without changing all of the blocks that come after it.

Because blockchain technology is decentralized, no single party has complete control over the network. Rather, through a consensus process, every participant, or node, has a copy of the complete blockchain and takes part in transaction validation. This

method increases transparency, lowers the possibility of fraud, and does away with the necessity for middlemen [11].

2.2 Blockchain's Evolution: Beyond Cryptocurrencies

Although the original purpose of blockchain technology was to facilitate the use of Bitcoin and other cryptocurrencies, during the course of the last 10 years, its potential uses have grown substantially. Blockchain is currently being used in a number of areas outside of finance, such as supply chain management, healthcare, voting systems, and the Internet of Things (IoT)[12].

Blockchain can be used, for instance, in supply chain management to follow the flow of goods from the producer to the customer, guaranteeing transparency and lowering the possibility of fraud. Blockchain ensures data privacy and integrity in the healthcare industry by securely storing and exchanging patient records. The tamper-proof record of transactions that blockchain offers makes it an invaluable tool for any application where transparency and trust are essential [13].

2.3 Dispersed Protocols and Consensus-Building Techniques

The use of consensus methods and decentralized protocols by blockchain technology to verify transactions and preserve the ledger's integrity is one of its fundamental characteristics. Consensus mechanisms are algorithms that, in the absence of a central authority, enable distributed networks to reach a consensus over the validity of transactions. The following are a few of the most popular consensus mechanisms:

The consensus method employed by Bitcoin and numerous other cryptocurrencies is called Proof of Work (PoW).. In proof-of-work (PoW), nodes, sometimes referred to as miners, compete to find solutions to challenging mathematical puzzles; the first to do so gets to add a new block to the blockchain. Although PoW is dependable and safe, it also consumes a lot of energy and has drawn criticism for its negative effects on the environment [14].

Proof of Stake (PoS): PoS is a PoW substitute that seeks to lower mining-related energy usage. The quantity of coins that nodes, sometimes referred to as validators, are ready to "stake" as collateral determines which nodes get to build new blocks in Proof of Stake (PoS). Many blockchain networks, including Ethereum 2.0 [15], employ Proof of Stake (PoS), which is thought to be more energy-efficient than Proof of Work (PoW).

Delegated Proof of Stake (DPoS) is a Proof of Stake variant wherein participants choose a limited group of delegates to approve transactions and generate new blocks on their behalf. The blockchain networks TRON [16] and EOS adopt this method since it speeds up transaction processing.

Practical Byzantine failure Tolerance, or PBFT, is a consensus technique that may withstand malicious node behavior and still function properly in the event of a Byzantine failure. For permissioned blockchains, when nodes are somewhat known and trusted, PBFT works especially well [17].

Table 1: Access Control in Centralized vs. Decentralized Systems

Aspect	Centralized System	Decentralized System
Authority	Single central authority	Distributed across nodes
Security	Single point of failure	No single point of failure

2.4 Smart Contracts and the Internet of Things

Self-executing contracts, or smart contracts, have the conditions of the contract explicitly encoded into the code. Without the need for middlemen, they automatically execute the terms of the contract when specific predetermined criteria are met [18]. In Internet of Things networks, where devices frequently need to communicate with one another independently, smart contracts are an effective tool for process automation.

In a smart home setting, for instance, a smart contract might be used to set the thermostat to change on its own when specific criteria are satisfied, like the time of day or the presence of people. Smart contracts have the potential to automate supply chain procedures in industrial IoT applications. For example, they may be used to order fresh materials when inventory levels drop below a predetermined threshold [19].

By eliminating the need for human intervention—which is frequently a weak point in security systems—the use of smart contracts in IoT networks can improve security. Furthermore, as smart contracts are stored on the blockchain, they offer a tamper-proof record of all transactions and interactions and are transparent and unchangeable [20].

3. IoT Networks: Challenges with Architecture and Security

3.1 IoT Architecture Overview

A vast range of networked devices, sensors, actuators, and communication technologies make up the Internet of Things (IoT), a dynamic and complex ecosystem. The main goal of the Internet of Things is to build a network where physical things can interact and communicate with one another as well as the surrounding environment to carry out a variety of functions on their own the perception layer, the network layer, and the application layer are the three general levels that make up the Internet of Things architecture [21].

The perception layer, sometimes referred to as the sensing layer, is made up of actual hardware and sensors that collect information from the surrounding world. These gadgets include basic RFID tags and temperature sensors as well as more sophisticated ones like GPS units and cameras. The perception layer's main job is to gather information and transform it into digital signals so that layer [22] can use it to communicate with other layers.

Network Layer: The network layer is in charge of sending the information gathered by the application layer to the perception layer. Networking and communication technologies including Wi-Fi, Bluetooth, Zigbee, and cellular networks are included in this layer. The cloud computing infrastructure, which offers processing and storage capacity for the enormous volumes of data produced by IoT devices [23], is another component of the network layer.

Application Layer: In the application layer, certain tasks are carried out by processing, analyzing, and utilizing the collected data. This layer, which encompasses a wide range of applications like smart homes, industrial automation, healthcare monitoring, and environmental monitoring, is in charge of providing services to end users. The application layer is extremely flexible and customized to meet the unique requirements of different industries [24].

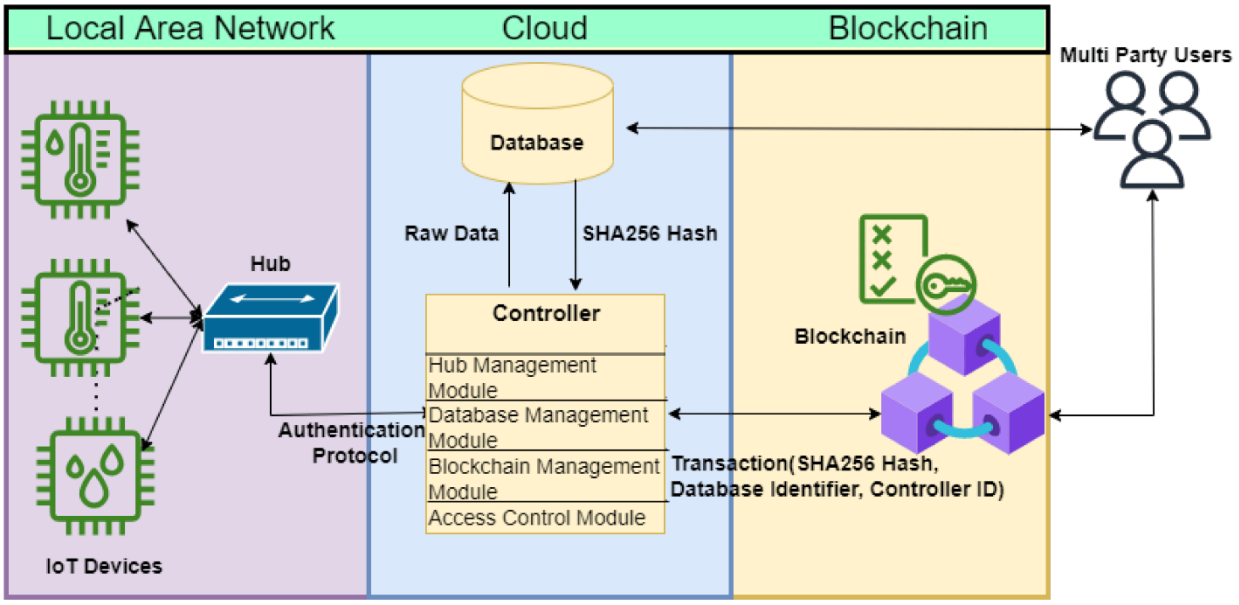

Fig 2: System Architecture

3.2 Common Security Threats in IoT Networks:

Because IoT networks are dispersed and interconnected, they are especially susceptible to a wide range of security threats. These dangers fall into a number of important categories:

Data Breaches and Privacy Violations: Internet of Things (IoT) devices are known to gather sensitive data, including location data, health records, and personal information. If this data is intercepted or accessed by unauthorized parties, it can result in serious privacy violations. Weak encryption, unsecure communication channels, and insufficient access control measures are common causes of data breaches in IoT networks. Distributed Denial of Service (DDoS) and DoS Attacks: DDoS attacks are more serious types of DoS attacks, in which a malicious actor uses multiple compromised devices—usually IoT devices—to overwhelm a target with traffic. DDoS assaults can be especially damaging in an IoT network because of the massive number of devices inside.

Botnets and Device Hijacking: Many Internets of Things (IoT) devices are built with few security features and little processing power. Because of this, malicious actors can easily take control of them and exploit the devices to create botnets. An attacker can remotely operate a network of compromised devices, known as a botnet, to perform coordinated attacks, such DDoS or spam campaigns.

Man-in-the-Middle (MitM) Attacks: In a MitM attack, two devices' communication is intercepted and maybe altered without the victims' awareness. As devices may be

sending sensitive data via unprotected channels in IoT networks, this kind of assault can be especially harmful.

Physical Attacks: Since many IoT devices are installed in the real world, they are susceptible to physical attacks, in contrast to traditional IT systems. In order to disrupt the network, these attacks may involve manipulating devices, removing confidential information straight from the hardware, or even destroying the equipment.

3.3 The IoT's Traditional Security Mechanisms' Limitations

Conventional security measures, while successful in protecting traditional IT networks, can prove inadequate in the context of Internet of Things networks. This insufficiency can be attributed to multiple factors:

Scalability Problems: Millions of devices can make up an Internet of Things network, and each one produces enormous volumes of data. This amount of data collection and device management is beyond the capabilities of traditional centralized security measures in terms of scaling successfully. The large amount of data might cause performance bottlenecks and increased vulnerability in centralized security systems.

Resource Constraints: Because many Internets of Things (IoT) devices are made to be small and affordable, their processing power, memory, and battery life are frequently constrained. Strong encryption and real-time monitoring are two examples of the security features that are challenging to install on individual devices because of these limitations.

Diverse and diverse Environment: The hardware, software, and communication protocols of IoT devices vary greatly, making IoT networks extremely diverse. It is difficult to apply a security solution that is appropriate for every situation due to this variability. Furthermore, the implementation of consistent security measures is made more difficult by the absence of standards among IoT platforms and devices.

Absence of Security upgrades: A lot of IoT devices are installed in settings where regular maintenance and upgrades are challenging because they are made for certain, long-term uses. These devices might not get security updates in a timely manner as a result, making them open to new attacks. Additionally, the lack of a reliable update mechanism allows known vulnerabilities to linger in IoT networks for a long time.

Latency and Real-Time Requirements: Low latency transmission and real-time data processing are necessary for certain Internet of Things applications, including industrial automation and healthcare monitoring. Time-sensitive IoT applications cannot benefit from traditional security measures since they can increase latency due to their frequent sophisticated processing and multi-layer encryption requirements.

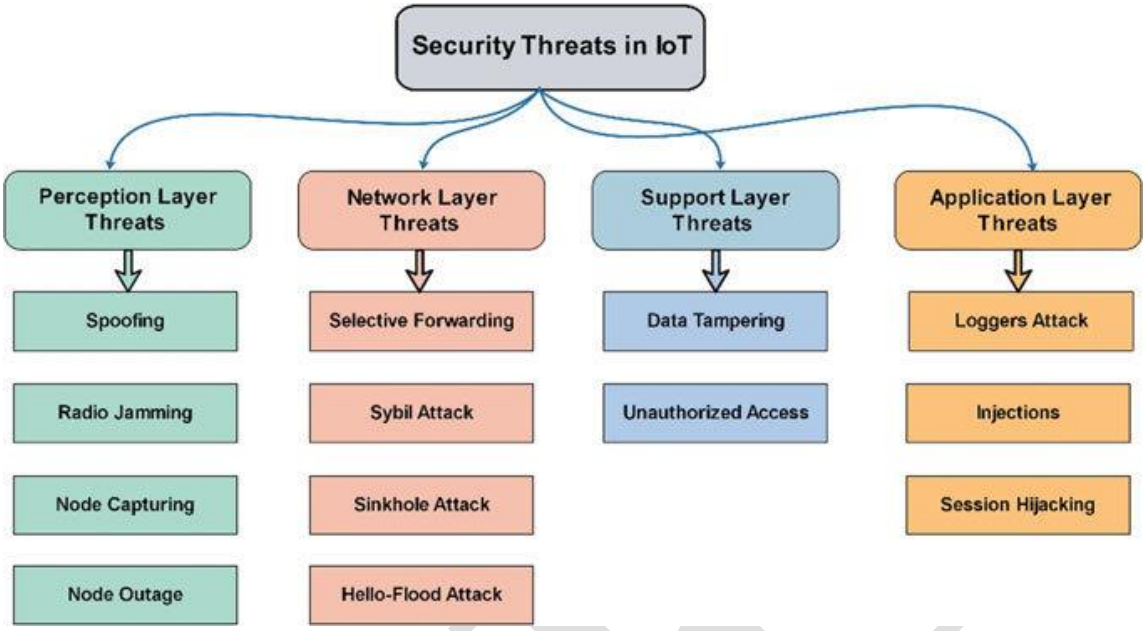

Fig 3: Security threats at different layers of the IoT architecture

4. Using Blockchain in IoT to Increase Security

4.1 Blockchain's Place in IoT Security

With its decentralized, immutable, and transparent properties, blockchain technology is becoming more widely acknowledged as a potent weapon for resolving the security issues that arise in Internet of Things networks. Blockchain lessens the risks linked to central points of failure, which are typical in conventional IoT architectures, by dispersing control throughout a peer-to-peer network.

Decentralization: One of blockchain's primary advantages is that it is decentralized, meaning that an IoT network's management no longer requires a central authority. Every device in an IoT ecosystem with blockchain support can function independently while keeping a safe and authenticated record of every exchange. Because of its decentralization, the network is more resistant to attacks and reduces the possibility of single points of failure.

Immutable Ledger: The blockchain's immutable ledger makes sure that once information is entered, it cannot be removed or changed without the network's approval. This feature is especially beneficial for Internet of Things networks, where data integrity is crucial. Organizations may guarantee that IoT data is accurate, unchangeable, and reliable by storing it on a blockchain.

Smart Contracts: Smart contracts have the ability to automate and enforce agreements between Internet of Things devices. They are self-executing contracts that have the contents of the agreement explicitly put into code. This feature improves network transaction security and lessens the need for human involvement. Smart contracts, for instance, can be used to govern access control, carry out transactions in accordance with preset criteria, and automatically authenticate devices.

4.2 Blockchain-Powered IoT Security Frameworks

To improve the security of IoT networks, a number of blockchain-based security frameworks have been developed. These frameworks take advantage of the special qualities of blockchain technology to tackle the particular security issues that IoT systems encounter.

4.2.1 Dispersed Access Control and Authentication

Conventional Internet of Things networks frequently depend on centralized access control and authentication systems, which can turn into weak points and targets for hackers. Blockchain provides a decentralized method of authentication that allows the network to independently verify each device. This method scales better with the growing number of IoT devices and enhances security as well.

For instance, devices are registered on the blockchain and their identities are confirmed using cryptographic techniques in a blockchain-based access control system. Smart contracts have the ability to encrypt access policies, guaranteeing that only authorized users or devices can access particular resources. By doing away with the requirement for a central authority to oversee access control, this approach lowers the danger of compromise.

4.2.2 Safe Data Exchange and Storage

Within Internet of Things networks, where sensitive data is frequently sent across numerous devices and platforms, secure data exchange and storage are vital concerns. Blockchain technology offers a transparent and safe method for data sharing and storage on Internet of Things networks. Every exchange of data or transaction is documented on the blockchain, resulting in an unchangeable audit trail that is simple to confirm.

Furthermore, blockchain technology can enable safe data exchange between various IoT network components. For example, information on the movement and condition of commodities can be safely recorded on a blockchain in an IoT supply chain system. Once authorized, this data can be exchanged without fear of tampering or unauthorized access with manufacturers, suppliers, and regulators.

4.2.3 Management of IoT Devices

It might be difficult to manage a large number of Internet of Things devices, as each one has different firmware, software, and configurations. By offering a decentralized and transparent platform for tracking device status, upgrades, and configurations, blockchain can simplify the management of Internet of Things devices.

Blockchain, for instance, can be used to track firmware updates, guaranteeing that every device connected to the network is running the most recent, safe software releases. A tamper-proof record of all actions conducted can be created by logging any modifications made to a device's settings on the blockchain. This transparency facilitates more efficient detection and handling of possible security breaches.

4.3 Blockchain-Enabled IoT Security Case Studies

4.3.1 Security of Smart Grids

Smart grids are especially susceptible to assaults because they incorporate IoT devices to optimize and regulate the flow of energy. The potential of blockchain technology to improve the security and dependability of smart grids has been investigated. Blockchain can help prevent illegal access to the grid, ensure safe transactions, and give a transparent record of energy usage and distribution by decentralizing control and utilizing smart contracts.

In one case study, a smart grid's blockchain-based platform was put in place to handle energy transactions involving many parties, such as producers, consumers, and grid operators. The system automated transactions depending on preset parameters, such supply and demand for energy, by utilizing smart contracts. This strategy decreased the possibility of tampering and eliminated central points of control, which not only increased the grid's efficiency but also increased its security.

4.3.2 IoT Security for Healthcare

IoT devices are being used more and more by the healthcare sector to handle medical equipment, keep track of patient health, and store private information. But there's a big worry about the security of these IoT devices since security lapses might expose private health data and cause essential medical services to be interrupted. Blockchain has been suggested as a way to improve the security of Internet of Things technologies in healthcare.

Blockchain was utilized in a case study concerning an IoT network for healthcare to protect patient data transfer between various devices and healthcare providers. The immutable record of all data transactions made possible by the blockchain made it impossible for patient information to be changed or accessed without the required authorization. Additionally, smart contracts were utilized to control data access, guaranteeing that patient records could only be viewed or altered by authorized personnel.

4.4 Blockchain's Drawbacks and Obstacles in IoT

Although blockchain has a lot of potential to improve IoT security, there are a few obstacles and restrictions that need to be taken into account.

Scalability: Proof-of-work consensus-based blockchain networks, in particular, may have trouble growing to large sizes. The network may get clogged as the volume of transactions rises, causing delays and higher expenses. In Internet of Things networks, where real-time data processing is frequently necessary, this might be a serious disadvantage.

Energy Consumption: In Internet of Things contexts where devices are frequently resource-constrained, the energy consumption of blockchain networks, particularly those that employ proof-of-work, can be an issue. Blockchain deployment in large-scale IoT networks may not be feasible due to high energy consumption, especially in situations where devices must run on limited power sources.

Interoperability: Blockchain integration faces a problem due to the heterogeneous nature of IoT systems and devices. A cohesive and safe network depends on ensuring compatibility across various blockchain systems and IoT devices. Attaining this interoperability can be challenging, though, especially in situations involving several suppliers and standards.

Cost and Complexity: Integrating blockchain technology into IoT networks can be expensive and time-consuming, especially for smaller businesses. Adoption may be hampered by the need to make considerable adjustments to current procedures and infrastructure in order to include blockchain technology. Furthermore, running and maintaining a blockchain network can be expensive, especially for small and medium-sized businesses.

5. Recap and Closing Remarks

In order to address important security issues, this research has looked at how blockchain technology can be integrated into Internet of Things (IoT) networks. We investigated how blockchain technology can improve several facets of Internet of Things security, such as device identification, data integrity, and administration, by utilizing its decentralized, immutable, and transparent features.

6. Results

Enhanced Security via Decentralization: The dangers associated with central points of failure in conventional IoT architectures are lessened by the decentralized nature of blockchain technology. This distributed method lowers the possibility of significant disruptions and increases resilience against attacks.

Immutable Data Records: IoT data is kept accurate and impenetrable by using blockchain technology for immutable data storage. This is important for applications like smart grids and IoT systems in healthcare where data integrity is critical.

Automation with Smart Contracts: Using pre-established rules and automatic execution, blockchain-enabled smart contracts can streamline operations and improve security by automating and enforcing agreements amongst IoT devices.

Limitations and Challenges: Blockchain integration in the Internet of Things (IoT) presents a number of obstacles, including interoperability, scalability, and energy consumption. It will take further study and development of compact and effective blockchain solutions to address these problems.

Future Directions: There are several interesting ways to enhance the security and effectiveness of IoT networks, including the use of quantum-resistant cryptography techniques, AI integration, and lightweight blockchain protocols. Furthermore, it will be essential to overcome ethical and regulatory issues if blockchain is to be widely used in IoT.

Table 2: IOTA Tangle Technology - Comparison with Traditional Blockchain

Aspect	Blockchain	Tangle (IOTA)
Data Structure	Linear chain of blocks	Directed acyclic graph (DAG)
Transaction Fees	Typically, present	No transaction fees
Scalability	Limited by block size and time	High scalability with no block size constraints
Transaction Speed	Can be slow due to block propagation	Fast, as transactions confirm each other

7. Techniques for Using Blockchain in Internet of Things

To ensure efficacy and integration, integrating blockchain technology into IoT networks requires a number of approaches and concerns. Practical methods such as blockchain frameworks, consensus techniques, and integration strategies are covered in this section.

7.1 IoT Blockchain Frameworks

Blockchain integration in Internet of Things networks require careful consideration while choosing the right blockchain architecture. For certain use scenarios, different frameworks provide differing features and performance attributes.

Ethereum: One of the most popular blockchain systems that facilitates decentralized apps (DApps) and smart contracts is Ethereum. Because of its adaptability, it's a well-liked option for Internet of Things applications that need automated procedures and programmable transactions. Nevertheless, large-scale IoT implementations may be constrained by Ethereum's scalability problems and high transaction costs.

Hyperledger Fabric is an open-source blockchain platform intended for usage in business settings. It is compatible with permissioned blockchains, which are more suited for private Internet of things networks where privacy and access control are essential. Modularity is a feature of Hyperledger Fabric that enables modification of data storage techniques and consensus algorithms, which can be useful for Internet of Things deployments.

IOTA: Specifically created for Internet of Things contexts, IOTA is a distributed ledger platform that resembles blockchain. It makes use of a structure known as the Tangle, which enables tremendous scalability, no transaction fees, and the removal of the need for miners. IOTA is suited for numerous IoT applications since its design is optimized for low-resource devices and microtransactions.

Another framework designed for use in enterprise applications is called Corda, and it was created by R3. In contrast to conventional blockchains, Corda directly logs transactions in a distributed ledger rather than grouping them into blocks. This architecture is a good choice for IoT networks that need to process data efficiently and with confidentiality since it lowers overhead and improves privacy.

7.2 IoT Network Consensus Mechanisms

Blockchain networks' scalability, security, and performance are all impacted by the consensus process selected. Many consensus approaches for Internet of Things applications are being investigated:

Proof-of-Work (PoW): Devices using Ethereum and Bitcoin must execute computational tasks in order to validate transactions. Although secure, its high computing needs and energy consumption make it unsuitable for IoT devices with limited resources.

Proof-of-Stake (PoS): Using their token holdings as a basis, players can validate transactions. Compared to PoW, this approach requires fewer resources, making it

more appropriate for Internet of Things networks where devices have limited computational capacity.

Delegated Proof-of-Stake (DPoS): In DPoS, delegates who approve transactions on the network's behalf are chosen by vote. This method increases efficiency and scalability, which makes it a good option for Internet of Things applications that need to process transactions more quickly and use less energy.

A consensus technique called Practical Byzantine Fault Tolerance (PBFT) is intended to manage errors and guarantee dependability in distributed systems. It can be modified for Internet of Things networks, in which nodes must come to a consensus in spite of possible malfunctions or malevolent actions.

7.3 Blockchain Integration Techniques for IoT

Blockchain integration into IoT networks needs to be carefully planned and carried out. There are several tactics that can help with this process:

Hybrid Approaches: By integrating blockchain technology with pre-existing IoT infrastructures, security and functionality may be gradually increased. For instance, while traditional systems perform less crucial duties, blockchain can be used for crucial services like data integrity and authentication.

Edge Computing: IoT network speed and scalability can be improved by combining blockchain technology with edge computing. By processing and validating data locally, edge devices can lighten the load on the core blockchain network and increase overall efficiency.

Interoperability Solutions: For a smooth integration process, it is imperative to guarantee interoperability between various blockchain platforms and Internet of Things devices. Creating common standards and protocols can let heterogeneous systems communicate and exchange data more easily.

Security Measures: You may improve the security of blockchain-based IoT networks by putting in place extra security measures like encryption, access control, and monitoring. By taking these precautions, you can guard against potential weaknesses and guarantee the network's integrity.

8. Conclusion

Blockchain technology offers a revolutionary solution for resolving security issues and improving the operation of interconnected systems when integrated into IoT networks. The decentralized, immutable, and transparent characteristics of blockchain technology can help IoT networks attain more security, efficiency, and trust.

The vital role that blockchain plays in Internet of Things security has been examined in this study, along with its applications in device management, safe data storage, and decentralized authentication. We have also looked at blockchain implementation techniques, such as framework selection, consensus methods, and integration tactics.

Looking ahead, the future of blockchain and IoT convergence will be shaped by developments in blockchain technology, new applications, and changing regulatory environments. We can create more intelligent, robust, and secure Internet of Things networks by taking advantage of new opportunities and resolving existing ones.

Ensuring that these technologies favorably contribute to the digital ecosystem and realizing the full potential of blockchain in the Internet of Things will depend on the ongoing research and development in this field.

References

[1] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, no. 2, pp. 6-19, June 2016.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks, vol. 54, no. 15, pp. 2787-2805, Oct. 2010.

[3] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," in Proc. Int. Conf. Comput. Sci. Electron. Eng., Hangzhou, China, 2012, pp. 648-651.

[4] M. Z. A. Bhuiyan, M. Safa, A. Gani, and R. Hasan, "Preserving Security and Privacy of IoT Applications in Smart Cities Using Blockchain Technology," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 906-918, April 2018.

[5] E. Bertino and N. Islam, "Botnets and Internet of Things Security," Computer, vol. 50, no. 2, pp. 76-79, Feb. 2017.

[6] M. H. Miraz and M. Ali, "Applications of Blockchain Technology beyond Cryptocurrency," Annals of Emerging Technologies in Computing, vol. 2, no. 1, pp. 1-6, Jan. 2018.

[7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146-164, Jan. 2015.

[8] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review," in Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl., Agadir, Morocco, 2016, pp. 1-6.

[9] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016.

[10] M. Pilkington, "Blockchain Technology: Principles and Applications," in Research Handbook on Digital Transformations, E. G. Carayannis, Ed. Cheltenham, UK: Edward Elgar Publishing, 2016, pp. 225-253.

[11] Y. Yuan and F.-Y. Wang, "Blockchain: The State of the Art and Future Trends," Acta Automatica Sinica, vol. 42, no. 4, pp. 481-494, April 2016.

[12] M. Swan, "Blockchain: Blueprint for a New Economy," 1st ed., Sebastopol, CA: O'Reilly Media, 2015.

[13] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital Supply Chain Transformation toward Blockchain Integration," in Proc. 50th Hawaii Int. Conf. Syst. Sci., Waikoloa, HI, USA, 2017, pp. 4182-4191.

[14] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, vol. 151, 2014.

[15] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2013.

[16] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 398-461, Nov. 2002.

[17] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A Distributed Solution to Automotive Security and Privacy," IEEE Commun. Mag., vol. 55, no. 12, pp. 119-125, Dec. 2017.

[18] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making Smart Contracts Smarter," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, Vienna, Austria, 2016, pp. 254-269.

[19] A. Gyrard, C. Bonnet, and K. Boudaoud, "Internet of Things Architecture Design Patterns," in Proc. 14th Int. Conf. Mobile Syst., Appl. Serv., Singapore, 2016, pp. 42-51.

[20] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," IETF RFC 7252, June 2014.

[21] R. Want, B. N. Schilit, and S. Jenson, "Enabling the Internet of Things," Computer, vol. 48, no. 1, pp. 28-35, Jan. 2015.

[22] L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," IEEE Trans. Ind. Inf., vol. 10, no. 4, pp. 2233-2243, Nov. 2014.

[23] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.