2026 Volume: 02 Issue: 06 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-24

BLOCKCHAIN AND INTERNET OF THINGS (IOT)

Samrity[1]*, Dr. Kamaljit Kaur[2]

[1]PhD Research Scholar, Sri Guru Granth Sahib World University Fatehgarh Sahib.

[2] Assistant Professor, Sri Guru Granth Sahib World University Fatehgarh Sahib.

Article Received: 5 May 2026

Article Revised: 26 May 2026

Published on: 16 June 2026

***Corresponding Author: Samrity**

PhD Research Scholar, Sri Guru Granth Sahib World University Fatehgarh Sahib.

DOI: https://doi-doi.org/101555/ijrpa.1294

ABSTRACT

'One of the most widespread technologies that was embraced by digital space is Internet of Things (IoT), which has altered digital space by providing connectivity of their smart devices to all industries of health, transportation, manufacturing, and energy systems. The combination of the Internet of Things (IoT) and the Blockchain technology has become a part of the entirely new array of concepts of creating the safe, open, and effective digital environments. In the chapter, the authors explore the application of Blockchain along with the IoT to address the primary challenges of data integrity, scaling, interoperability, privacy, and energy efficiency. It focuses on the various types of Blockchain designs, i.e. a public, a private and a consortium that complements the decentralized IoT models with an unalterable data tour, without trust communication and smart contract implementation. The discussion also broadens the subject of consensus mechanisms in Internet of Things including lightweight and hybrid schemes, which make the most use out of resources. IoT solutions facilitated by Blockchain have been practically applied in medical practice, supply chain, smart cities and industrial automation to denote the newfound importance of IoT solutions. The chapter concludes with the identification of the new research patterns, technical concerns, and a way of moving to make Blockchain and IoT sustainable, secure, and smartly developed ecosystems.

KEYWORDS: Blockchain, Internet of Things, Decentralization, Consensus Mechanism, Smart Contracts, Data Security, Energy Efficiency, Interoperability, IoT Applications.

1. INTRODUCTION

Internet of things (IoT) has become one of the most significant digital transformations that allow connecting billions of smart devices in many aspects, such as healthcare, transportation, manufacturing, and energy capital.

This is the power of the IoT as it will be able to change raw into actionable knowledge by connecting devices, sensors, and applications to provide adaptive and responsive environments.With the development of the Internet of things (IoT), many fields have altered the healthcare, transportation, manufacturing, and energy among others through their interconnecting of billions of intelligent devices and the ability to exchange data in real time. Nonetheless, conventional architectures have significant threats in the areas of data integrity, security, scalability, interoperability, privacy, and energy-efficiency. The decentralized and immutable ledger of blockchain technology has become one of the most effective solutions to most of these issues, and a new era of the emergence of safe and transparent digital ecosystems has begun.

As IoT devices keep on increasing, there are inherent security, scalability, efficiency and interoperability issues with the conventional centralized architectures. Being known by its decentralized, immutable, and transparent data management, blockchain technology has become a prospective solution to these issues and provide safe and efficient IoT frameworks.[1].

Here is an increasing merge of blockchain with IoT systems:

Enhanced Security and Trust

Blockchain's Immutability: The blockchain ledger immutability hints toward a decentralization method capable of securely preserving InternetofThingsdata, assuring the integrity of the information stored.

Reduced Single Point of Failure: In regard to the decentralized blockchain architecture, the number of nodes reduces the susceptibility to a point of failure attack, thereby leading to a more robust system better suited for many IoT networks when compared to centralized blockchain systems.

Trustful Sharing of Data: The blockchain will allow sharing sensitive information among various stakeholders and enhancing the visibility and responsibility of nonhomogeneous IoT systems.

Enhanced Data Transfer: With the integration of blockchain technology, the Internet of Things (IoT) devices have a lot of potential to improve the speed and the efficiency by which

data is transferred within systems and improve the operation of the systems while lowering the waiting time.

Traceability and Provenance: Using blockchain technology, it is possible to track the complete history of every piece of data and thus increases the transparency and the traceability across the complete life cycle of the data.

Automation of Contracts: Using predefined conditions, business processes and workflows can be automated using Smart contracts which allows the assets to be utilized fully, reduces the need for human input and the processes to be performed optimally.

Addressing IoT Challenges

Scalability: The ability of the Blockchain to be decentralized can enhance scalability in the IoT networks and it enables a large number of connected devices to be handled.

Data Security and Privacy: Blockchain encryption and access control would help deal with the issue of security and privacy of IoT data.

Interoperability: Blockchain will be able to provide interoperability among various IoT smart devices and systems allowing a smooth flow of data and entry.

Industries to which it can be used include:

Supply Chain Management: Blockchain will have the ability to follow the goods supplied within the supply chain making sure that the goods are genuine, less fraudulent, and efficient.

Healthcare: Blockchain has the potential of securing patient data, facilitate secure data sharing among healthcare providers, and ensure remote patient monitoring.

Smart Cities: The blockchain is capable of handling the data of smart grids and enhancing traffic flow and the safety of the people in the smarter cities.

Production: Through blockchain, it is possible to identify the goods and ingredients, simplify the operation, and guarantee quality.

The chapter discusses the convergence between blockchain and IoT. It examines blockchain design options (public, private, and consortium), the review of consensus mechanisms specific to the IoT setting and current challenges.

2. FUNDAMENTAL OF BLOCKCHAIN AND IoT

2.1 Internet of Things

IoT networks are physical devices which are fitted with sensors, actuators and communication interfaces in smart homes, vehicles, kitchen and home appliances. These are used to collect and send data on data monitoring, analysis and control processes and are

autonomous. Although IoT transforms the data collection, decision-making process, and automation, the conventional centralized approach of managing it creates vulnerabilities, i.e. one point of failure; vulnerability to security attacks.

Layers of Internet of Things (IoT)

IoT works in three core layers namely as perception, network, and application [2].

These layers provide security in ensuring that the information that has been gathered by the devices is relayed safely and utilized efficiently to make decisions.

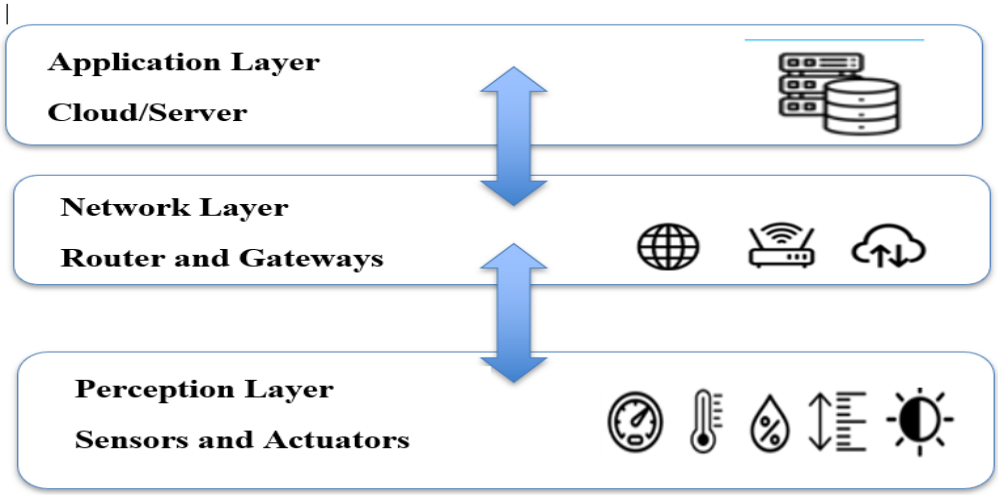

Fig: 1 core Layers of Internet of Things(IoT)

Perception Layer: This layer is a physical layer, which is made up of all the sensors, actuators, and other edge devices of the IoT, which gather data of the environment (temperature, motion, or health parameters).

Network Layer: Involved in the sending and receiving of the information gathered by the perception layer to the areas where necessary processing or storage devices such as Wi-Fi, Bluetooth, ZigBee and different gateways; in addition, it also facilitates the connection of devices and provides security to data when transferring it.

Application layer: Services and user interfaces Application layer provides the use of IoT data to provide results through analysis and processing and offering application services through smart homes, healthcare, control over industrial automation, and others.

The IoT devices generate massive amounts of information and this travels through the use of networks. There are only devices that attempt to store information in the actual form otherwise all will make some modification with the information.

Information available in the Internet of Things can be:

- A person with a heart monitor,
- The farm animal should have a tracking chip, which will check its health,
- A vehicle that will warn the owner of a low-tire pressure,

This is any item that has the capability to access the internet and transfer data.

Nevertheless, IoT is associated with centralization issues, susceptibility to hacking, and non-interoperability of systems between platforms [3].

2.2 IMPORTANCE OF IOT

The significance of the Internet of Things (IoT) is in its capacity to associate the daily items with the web enabling them to obtain, transfer, and handle data to enhance effectiveness, mechanization, and decision-making in different fields. IoT will improve its productivity, decrease its manual labor and error, allow real-time monitoring, help in saving costs and lead to innovation in personal, industrial and health care fields.**Increased productivity and low operational costs**: IoT automatizes functions and maximizes the efficiency, which means improved productivity and low operational costs. This cuts down the human factor and manual work as well as allows making intelligent decisions based on information.

Real-Time Monitoring and Control: IoT devices can give real-time data on environments, equipment, or health related conditions, allowing timely response to enhance the safety of environments and equipment, eliminate downtime, and streamline resource utilization. Remote patient monitoring enhances emergency services and personalized care in the sphere of healthcare.

Business and industrial Impact: IoT is used to streamline production processes, stock management, and forecasting maintenance demands in the industry and driving cost reductions and productivity enhancement. It is also applicable in supporting new business models and competitiveness through physical and digital integration.

Personal and Health Goodes: IoT wearables and smart devices will allow individuals to learn more about their health condition and automatize the house management processes, improve the quality of life and keep themselves safer.

2.3 BLOCKCHAIN TECHNOLOGY

The blockchain technology is a state of art database mechanism which ensures release of transparent information to the business networks. A blockchain database stores information in

nodes which are connected together in a chain. The information is time-based inflexible as you cannot erase or alter the chain without the consent of the network.

Blockchain technology is adopted in the development of an immutable or resolute registry to trace orders, payments, accounts, and other dealings. This system has incorporated protections, which ensure that transactions are not entered illegally and introduce consistency to the shared opinion of transactions.

Blockchain is a decentralized registry based on the technology that allows recording, sharing, and synchronization of data between autonomous participants. The main features of it are the immutability, transparency, and decentralization and the possibility of automation with the help of smart contracts.

Blockchain is a distributed registry technology that is adopted to document transactions in unambiguous, verifiable, and decentralized form. All the blocks include their cryptographic hash of the previous block, which provides integrity of the data [4]. Decentralization, immutability, transparency, and security of Blockchain are its fundamental aspects that render it an appropriate background of the distributed IoT data management. Consensus mechanisms like Proof of Work (PoW), Proof of Stakes (PoS) and Practical Byzantine Fault Tolerance (PBFT) are used in the validation and consent of the network nodes [5].

2.4 ELEMENTS OF BLOCKCHAIN TECHNOLOGY

Consensus: It provides the proof of work (POW) and verifies the activity in the networks.

Ledger: It provides complete details of the transactions in the networks.

Cryptography: It makes sure that all data in ledger and networks get encrypted and only permitted users can decrypt the data and information.

Smart Contract: It is principally applied to verify and confirm the members of the network.

TYPES OF BLOCKCHAIN TECHNOLOGY

Blockchain networks may be:

Public (unauthorized, open to everybody)

Privatized (limited to a central authority).

Consortium (managed by association of organizational stakeholders)

Hybrid (managed by one entity with some policies)

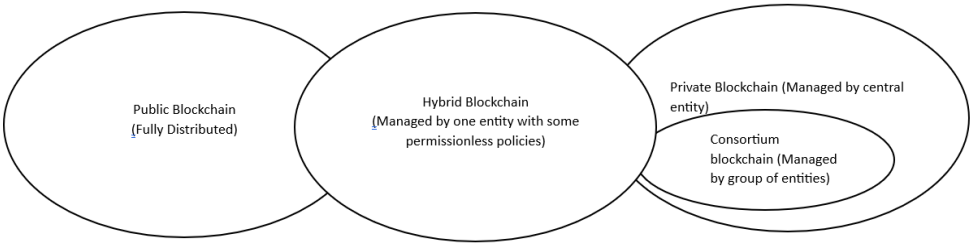

Fig 2: Blockchain Types.

Public Blockchain: A public Blockchain is also referred to as a permissionless Blockchain, and is completely transparent to any participant and is a completely decentralized Blockchain. Each node is permitted to add and mine the new blocks of transactions equally. Some of the most well-known examples of publicly available Blockchain platforms are Bitcoin and Ethereum.

Private Blockchain: Private Blockchains are commonly implemented in cases where businesses want to have full control over their solution based on Blockchain. Such organizations are capable of establishing privileged access and engagement in the agreement procedure. Authorized or private Blockchains are more secure in nature and there is no necessity to have massively complicated cryptography calculations when verifying blocks.

Consortium Blockchain: Consortium blockchains refer to a form of a special category of private blockchain. Consortium blockchains have a group of organizations rather than being operated by one organization like it is in the case of the private blockchains. The blockchains are usually applied to supply chain management and other interoperative industries.

Hybrid Blockchain: There are significant flaws in both the public and the private blockchains. An example is that public blockchains may be highly delayed in the validation of blocks whereas private blockchains are also usually more centralized and are therefore more susceptible to disruptive elements aimed at their blockchain managing organizations. In order to have the merits of both forms of blockchains (public and private), hybrid blockchains are also invented.

2.5 CORE COMPONENTS OF BLOCKCHAIN

The functioning of blockchain technology was based on a node -computer network through which the distributed ledger is maintained and validated. These nodes are in various varieties; full nodes, which contain full copies of the blockchain, lightweight (also referred to as nodes having only transaction hash copies), and mining (that authenticate new transactions and add

them to the blockchain). The blockchain itself is a distributed registry, which may be a public system, accessible by anybody, or a privatized system, which has all of the nodes holding synchronized copies of the database in a decentralized system. Consciousness is established in a number of ways such as Proof of Work (in the case of Bitcoin), or Proof of Stake (in Ethereum 2.0), and all the nodes are sure about the correctness of the transactions. Data integrity is secured by cryptographic principles, such as hash functions, and authenticity of transactions is checked by using cryptographic principles (digital signatures). It remains an infrastructure that enables smart contracts as self-executing contracts that automatically handle transactions in the event that specified conditions are met, in the range of applications in different industries such as supply chain management to decentralized finance. Below Figure Describes the core components.

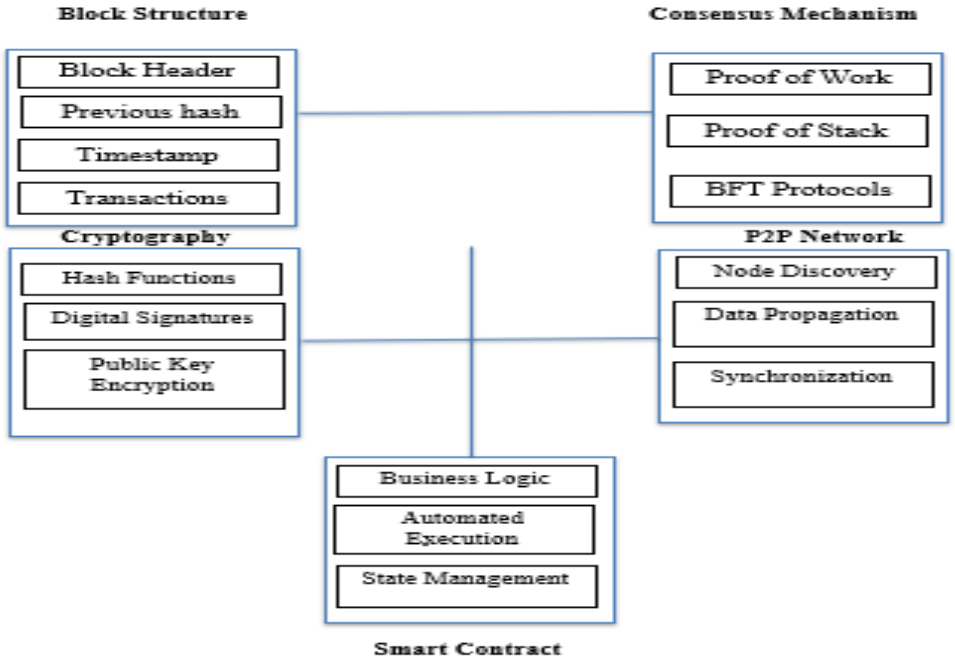

Fig 3 : Core Components.

The technology of blockchain has grown way past the use of cryptocurrencies. It has now been used in a variety of use cases such as smart contracts, supply chain management, cybersecurity and verification of data integrity. The most notable advantages of the technology include its universal availability, incorruptibility and capability to save and transmit all forms of valuable information or transaction history safely without third parties.

2.6 IMPORTANCE OF BLOCKCHAIN

Greater Protection and Data Integrity: Protection of data is one of the essential contribution factors of blockchain which enhances an unprecedented security level. The data once put into a blockchain is almost impossible to amend or remove. This imparts the level of permanence which sets the information that is documented as credible and immune to manipulation. Blockchain has offered a solution that is very much required in areas where the integrity of the data matters like in the financial sector, health sector, and supply chains of goods and services.

Transparency and Trust: Blockchain allows transparency or makes transactions transparent to all network members. Every transaction is stored in a public ledger that can be verified by anybody and this makes transactions trustless. This implies that they do not require intermediaries such as banks and brokers to be able to check on transactions. The blockchain also, in its turn, helps implement the attitude of trust between parties that would not have previously been involved in any such relationships, eliminating the necessity to have a third party and risks of fraud.

Decentralization and Disintermediation: Traditional systems tend to be centrally controlled to undertake transactions or processes providing bottlenecks and points of failure. This is done away with by blockchain through the decentralization of the network. There is no centralized authority and this reduces the chances of wide-scale failures or corruptness of the system. Also, blockchain facilitates the concept of disintermediation whereby intermediaries are eliminated. This is especially the case in such industries as finance where middle-men such as banks can slack processes and generate other charges. Blockchain will simplify transactions and lowers expenses and enhances efficiency by eliminating these middlemen.

Economy and Time: Within the traditional systems, transactions that are involved in the processing system may take time and cost because of the manual checks, verification and third-party participation. Blockchain, though, makes these processes automated, by implementing smart contracts, which are self-executing contracts in which the terms are coded. The contract automatically becomes effected after satisfying a set of predetermined requirements without the requirement to involve a human component. This is not only quickening the process of the transaction, but also saves operation cost, which makes blockchain a very viable tool in the case of a business that wants to streamline its performance.

The Innovation Catalyst: Blockchain is driving change, not just in its direct use, but overall, in the industry. Examples include the use of blockchain in supply chain management to keep

track of the goods produced to consumer, and detect authenticity and minimize counterfeiting. In the health sector, it is enhancing data safety through the establishment of a decentralized and secure pool of patient data. The fact that blockchain can manage the multi-step and complex procedures with transparency and security is providing an innovation and disruption opportunity.

3. NEED FOR INTEGRATION OF BLOCKCHAIN AND IoT

The combination of both Blockchain and IoT is a groundbreaking move that would amount to the development of safe, transparent, and autonomous digital systems. IoT networks are made up of billions of inter-connected physical entities, i.e. simple sensors and industrial control system, which constantly generate and transmit information. Nevertheless, conventional centralized architectures to handle IoT data are severely limited, such as being susceptible to single point of failure, vulnerability to data manipulation and scalability [6]. The blockchain technology is capable of dealing with these obstacles due to the decentralized system that is able to establish distributed trust, resistant data storage, and automated transactions due to the smart contracts [7].

Decentralized Data Management: The traditional IoTs have most information being processed and stored in central cloud computers. The model introduces possible bottlenecks in access, storage and security of data. Blockchain eradicated these weaknesses by spreading the ledger to a number of nodes on the network. The ledger is replicated in every node so that the integrity of data cannot be destroyed in the case when some of the nodes become inactive or malfunction [6]. Such decentralization will provide fault tolerance and avoid the illegal modifications of IoT data. Consequently, Blockchain implementation offers immutability and verifiability, which are the required properties on life-and-death IoT applications, e.g. healthcare monitoring, industrial automation, and tracking shipments.

Smart Contracts Automation: Smart contracts are automated scripts that are stored in the Blockchain and can perform a set of automated activities upon the fulfillment of specific conditions. In combination with IoT, smart contracts enable the devices to make timely transactions and implement decisions without the involvement of the human [7]. An example of this is a smart energy meter which can automatically make payments to a supplier when some maximum amount of energy is used, or an automated paid car pay a toll based on the data of GPS location. This degree of automation does not only enhance efficiency in the operational capacity, but also, third party intermediaries are missed out, thus saving costs and latency as well.

Improved Security and Data Integrity: Since IoT ecosystems are both distributed and heterogeneous, security has been a major concern therein. The introduction of blockchain makes the IoT solutions more secure with the help of cryptographic hash, digital signatures, and decentralized authentication. Every single transaction hourly recorded in the Blockchain is encrypted and confirmed by several nodes prior to being stored in the ledger and thereby data tampering is not a possibility [6], [11]. Moreover, cryptographically secured identities can ensure the protection of the IoT equipment against malicious attacks and attacks to impersonation, as the firmware updates can be secured with Blockchain to guarantee that only an authorized person can access the equipment.

Trustless device to device communication: A common IoT network sees devices being connected to centralized gateway or cloud server based communication. This dependence may lead to setbacks and confidentiality of data. Blockchain facilitates peer to peer (P2P) communication, with the IoT devices able to communicate and exchange information with each other through a trustless consensus model [12]. This not only minimizes latency but also ensures improved efficiency in communication and gets rid of the centralized authentication authorities. Through a clear and indelible transaction record, Blockchain ensures that the interactions of the devices could be inspected and confirmed and accountability is promoted in an intricate multi-device setup.

Interoperability and Data Sharing: Interoperability of the devices of various manufacturers is one of the challenges which has continued to haunt the IoT systems. Blockchain offers a seamless data sharing platform across the domains, where cross-domain data may be shared safely and standardized, across a heterogeneous device and network [9]. The given ability comes in especially handy in applications on a large scale, like smart cities or supply chain management, in which several parties should exchange real-time information safely. The decentralized system of blockchain helps to foster inter-organizational trust to allow sharing sensitive information without jeopardizing confidentiality.

Energy Efficiency and Lightweight Protocols: Conventional Blockchain architectures such as Bitcoin and Ethereum use high computing power and are therefore not suitable to use in IoT devices that are resource limited. In order to address this drawback, lightweight consensus algorithms are used that include Proof of Authority (PoA), Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT) as methods to enhance energy efficiency and minimize latency [11], [12]. It has been especially created to be used in the IoT applications whose transaction throughput is large, with limited processing power. There is also potential in having emerging hybrid models which would integrate various consensus

algorithms and realizing optimal trade-offs in the framework of security, scalability, and performance.

4. SOLUTIONS FOR THE ISSUES OF IoT AND BLOCKCHAIN

The key challenges of the integration of the IoT and blockchain are the scalability, energy consumption, security and privacy, compatibility/interoperability, latency, and resource constraints of the IoT. The solutions to these problems include a combination of tech changeover and architecture:

Use Permissioned or Lightweight Blockchains: Permitted blockchain models such as Hyperledger Fabric use overhead blocked blockchains to reduce blockchain overhead on IoT devices.

Layered Architectures: The IoT is loosely coupled to the blockchain, and the storage contains blockchain-verifiable data that may be stored off-chain using layer-2 storage solutions (Lasrado, 2020).

Consensus Algorithm Optimization: In some cases, a consensus algorithm can be optimized, e.g. by using an energy-efficient consensus algorithm (e.g. Raft, Proof of Authority) in place of an energy-intensive Proof of Work.

Privacy Improvements: Implement zero-knowledge proof methods and in encryption methods (e.g., zkLedger) as a way of safeguarding sensitive IoT data on blockchain.

Edge Computing: handle the data locally at one of the edge devices to save on the latency and blockchain load.

Interoperability Protocols: Work on standards and middleware to facilitate free communication among different devices on the IoT and connect them with the blockchain networks.

Automation with Smart Contracts: Automate diminishing error rates and increasing stability in transactions by using smart contracts to automate device management, authentication, and safe transactions.

Frequent Firmware and Security Upgrades: Additional security is constantly applied to IoT devices with upgrades and blockchain authentication of devices.

5. SUITABILITY FOR IoT

The blockchain technology has been deemed to be applicable in the applications of Internet of Things (IoT) since it has been found to complement security, data integrity, transparency, and trust in a decentralized way. It offers immutable records of transactions that are tamper-

resistant which may enhance authentication of devices, facilitate autonomous and secure communication between devices through smart contracts and eliminate the need to use centralized authorities. These aspects can help overcome the significant IoT challenges such as data privacy, reliability, and scalability, as well as ease the automated and efficient management of devices. The option will be based on the application scenario. The majority of IoT uses would choose either private blockchain or consortium blockchain because of:

(a) high throughput required

(b) low latency required.

(c) Sensitive data management

(d) regulatory compliance

5.1 BLOCKCHAIN ARCHITECTURE FOR IoT APPLICATIONS

Incorporating the Internet of Things (IoT) systems with the effective infrastructure of the Blockchain technology requires the prevalence of the specific Blockchain system. All Blockchain architectures, such as the public, the private, and the consortium, have different characteristics, accessibility, and different types of governance that shape the process of data exchange, verification, and storage of IoT devices [8], [9]. The correct choice of the architecture is also essential to realizing a favorablecompromise between the security, scalability, decentralization, and performance of IoT systems in a resource-constrained environment.

Public Blockchain: A Public Blockchain is a thoroughly decentralized and permissionless blockchain in which any participant can join, verify and contribute towards the blockchain. The examples are Bitcoin and Ethereum which make use of consensus mechanism like Proof of Work (PoW) and Proof of Stake (PoS) to confirm the transactions [8]. Transparency and immutability are the most crucial capabilities of public Blockchains in IoT systems, as they guarantee that the interaction between all the devices could be verified by any node in the network.

Nevertheless, the public Blockchains lack scalability, have latency, and consume large quantities of energy, which is essential in the environment of the IoT when a device is often resource-constrained [11]. As an example, having a smart sensor network connected to Ethereum could lead to the delays of the transactions validation process because of the inadequate throughput. Thus, transparent and auditability applications like the energy trading of smart cities or open data registries should be better implemented on public Blockchains [10].

Private Blockchain: A Private Blockchain has a permissioned model in which any external party is not allowed to access the blockchain unless it is a part of an authorized organization or a defined ecosystem. This is in contrast to public Blockchains as in private architectures the cryptographic immutability and tamper-resistance is maintained although centrally controlled [9]. The model best suits the IoT scenario in industries, where crucial information like manufacturing history or work metrics should not leak out.

Hyperledger Fabric or Multichain are seen as examples of Private Blockchains where the administrators can set up the rules of participation, the visibility of the transaction, and the set of the consensus parameters. This flexibility gives them a good fit to enterprise level IoT systems which require a level of controlled access, low latency and high throughput [10]. Moreover, an infrastructure based on edge computing can be combined with a private Blockchain since it can be performed near IoT devices, thus minimizing the latency and consumption [14].

However, with private Blockchains, there is some form of centralization and thus, this could undermine the decentralized spirit of Blockchain. That is why, they are typically implemented in the environment where the level of trust between the players is already partially built, and the privacy of data has higher priorities in comparison with transparency requirements.

Consortium Blockchain: Consortium Blockchain is also known as a federated Blockchain is a hybrid solution that is a combination of the merits of open and closed structure [10]. In a consortium Blockchain, several pre-defined nodes or organizations run and control the other nodes as opposed to one. The validation process ensures that every member is involved in the process allowing shared governance, accountability, and trust not to be fully centralized.

The model is especially applicable in multi-stakeholder IoT scenarios, including healthcare networks, smart logistics systems, energy trading platforms, and others, in which several parties should exchange and authenticate information safely [9]. As an illustration, in the supply chain based on a Blockchain, manufacturers, distributors, and retailers can mutually validate the provenance of products guaranteeing the transparency and authenticity of the process [14].

Table 1: Comparative Analysis

Feature	Public Blockchain	Private Blockchain	Consortium Blockchain
Access Control	Permissionless	Restricted to single organization	Restricted to selected group
Decentralization	Fully decentralized	Partially centralized	Moderately

			decentralized
Transaction Speed	Low	High	Moderate to high
Energy Efficiency	Low	High	High
Transparency	Complete	Limited	Controlled
Suitability for IoT	Public data-sharing systems	Industrial IoT	Multi-party IoT ecosystems

Efficient consensus-making schemes that are standard with Consortium Blockchains are Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA) that offer increased processing of transactions in less energy use than PoW [11]. Moreover, this model provides the ability to maintain data privacy, scalability and performance, which means that it is a promising architecture of the IoT ecosystems in the future.

As shown in Table 1, public Blockchains are best suited for open, large-scale IoT networks, while private and consortium architectures are preferred for enterprise and collaborative IoT ecosystems that require controlled access and higher performance [8], [9].

5.2 NEW HYBRID ARCHITECTURE

Recent developments on research point out the development of hybrid Blockchain constructions, that is, seek to exploit the advantages of the different models collectively [12]. Such systems can use either public Blockchains to verify their data and private or consortium to conduct their transactions and store their data. These hybrid systems enhance scalability and privacy of data as well as interoperability in various settings of the IoT.

It is also observed that hybrid structures are being increasingly combined with edge computing and cloud computing to enable real-time data processing nearer to IoT devices with the use of the Blockchain to secure data validation. This makes the system more efficient and resistant, which is why this is one of the most prospective directions of large-scale IoT implementation.

6. CONSENSUS MECHANISMS FOR IoT NETWORKS

The conventional Blockchain consensus mechanism tends to be resource-consuming, which makes it difficult to put IoT devices with low computational power. Lightweight protocols include, but are not limited to, Proof of Authority (PoA), Delegated Proof of Stake (DPoS) and Directed Acyclic Graph (DAG) based model by improving scalability and minimizing energy usage [11]. Hybridization between these mechanisms is becoming popular to maintain a tradeoff between efficiency and security [12].

6.1 CONVENTIONAL CONSENSUS ALGORITHMS

Broadly used blockchain protocols such as Proof of Work (PoW) and Proof of Stake (PoS) are resource-intensive, and are not practical on IoT devices with limited resources in terms of computing capabilities and energy costs.

Proof of Work (PoW) is employed to pick a miner to be used in producing the next block. This is the PoW consensus algorithm of Bitcoin. The main principle of this algorithm consists in solving a complicated mathematical riddle and providing one with a ready answer.

Proof of Stake (PoS) is the most common alternative to PoW. Ether has moved away in PoW to PoS. Rather than spending money on purchasing costly equipment to crack some sort of a puzzle, the validators in such a consensus algorithm spend on the coins of the subjects by locking up part of their coins as collateral. Then, all the validators will begin to validate blocks. The validation of blocks will be done by the validators making bets on it in the event that they find a block which they are certain can be added to the chain. Depending on the real blocks introduced in the Blockchain, all the validators receive a reward in proportional amounts of their bets, and their stake multiplies correspondingly. Finally, a validator is selected to produce a new block depending on his or her economic interests in the network. PoS, therefore, provides incentives to validators in order to come to an agreement.

6.2 LIGHTWEIGHT AND HYBRID CONSENSUS MECHANSMS

Proof of Reputation (PoR) Provides energy efficient and fast consensus based on trusted registers. This makes use of the resources available in the IoT devices to achieve consensus, which improves energy efficiency and scalability of sensor-intensive environments.

Proof of Authority (PoA) Relies on the identity and reputation of validators to provide a faster transaction and reduce computational needs.

Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm that was suggested by Barbara Liskov and Miguel Castro in the late 90s. PBFT was aimed at operating effectively in asynchronous (there is no maximum limit on the time when the response to the request will be available) systems. It is optimized with respect to low overhead time. It aimed at addressing most issues with Byzantine Fault Tolerance solutions that were in existence.

Delegated Proof Of Stake (DPoS) is also a variant of Proof of Stake consensus algorithm. This kind of consensus mechanism is based on the foundation of the delegation of votes. The users delegate their votes to other users. The rewards will be shared out to the users who delegated to the vote that is mined by a particular user by whichever user then mines the block.

Proof of Burn (PoB), PoB, rather than investing in costly hardware equipment, validators burn coins through the transfer of coins to an address that coins can never be recovered. Validators are granted the right to mine on the system by committing the coins to an inaccessible address by the selection process which is randomly selected. Then, to burn coins, in this case, is a long-term commitment of the validators in return of their short-term loss.

Proof of Capacity validators are also expected to invest their hard drive space rather than invest in a costly hardware or bitcoin burning. The higher the validators capacity of the hard drive, the higher the possibility of being picked to mine the next block and attain the block reward.

Proof of Elapsed Time (PoET) is one of the fairest consensus algorithms that select the next block in a fair manner alone. It is extensively applied in authorized Blockchain chains. Each validator in the network receives a balanced opportunity to make his own block in this algorithm. Each of the nodes does this by randomly delaying the time by adding evidence of the delay to the block. The blocks generated are sent to the network to be taken into account by other people. The winner is the one that has the least time in the proof section. A winning validator node appends the block it has to the Blockchain.

Hybrid Mechanisms: There are IoT blockchain systems that use a combination of consensus protocols (e.g., PoS, PBFT) to scale the consensus protocols to requirements of healthcare applications without compromising on one or the other.

7. APPLICATIONS OF BLOCKCHAIN ENABLES

IoT systems are becoming more and more actively implemented in different fields that are supported by blockchain. Blockchain can protect patient records in health care and also guarantee data integrity [13]. It is used in supply chain management to make the supply chain more transparent and traceable of its products [14]. Blockchain is utilized in Smart city models to manage energy, share of data and safety of the population [15]. The senses of secured machine-to-machine communication and proactive maintenance brought by the Blockchain-IoT integration would serve as a benefit of industrial automation [16].

Healthcare Systems: The integration of Blockchain and IoT in healthcare delivery is becoming more popular within healthcare systems as a method to provide security of data, privacy of patients, and the overall interoperability of medical equipment and electronic health records (EHRs). Medical devices that utilize IoT constantly gather sensitive information, including heart rate, glucose levels, and blood pressure that are sent to make a diagnosis and observe them. Nevertheless, conventional centralized health information

systems have a tendency of data leakage and breach of unauthorized access. Blockchain also will provide safe and unalterable storage of patient data meaning that only authorized users (e.g., physicians, insurers, and patients) can access records with cryptographically secure smart contracts [13]. As an example, the information in wearable IoT devices can be hashed and stored in the Blockchain after each processing, which will ensure its authenticity and traceability. Moreover, the use of a consent management system based on the concept of the Blockchain allows patients to control the access of the medical information and guarantee the privacy and regulatory factors (e.g., HIPAA and GDPR). The implementation that is worthy of mentioning is the MedRec framework that operates Ethereum smart contracts to securely share patient identities and medical records among healthcare providers [13]. IoT with the blockchain, therefore, raises the level of reliability, interoperability, and trust of contemporary healthcare ecosystems.

Supply Chain and Logistics: Traceability, anti-counterfeit operation, and inter-participation are some constant issues that supply chain systems face. The IoT solutions enable by the use of blockchain will resolve such problems because each movement of products and transactions will be recorded with uncertainties, providing final tracking of the product throughout the whole supply chain, this means it will start at manufacturing processes and continue to the end-user [14]. The IoT sensors and RFID tags placed on the goods collect the data on the location, temperature, and humidity and release them to the Blockchain to be verified. Such combination allows to perform real time monitoring and provenance tracking, preventing fraud and securing product authenticity. The Food Trust project in Walmart and IBM, is an example of a system with a combination of Blockchain and IoT to identify the origin and solitude of food products and minimize the time needed to determine the cause of contamination by a large margin [14]. The model has the benefit of removing counterfeit drugs in the pharmaceutical industry since the origin of products has been verified at each point in the supply chain. In addition, smart contracts make it possible to make automated payments and verifications of shipment in case of fulfilling conditions (e.g., a package arrived at a certain location or temperature). This automation enhances the transparency, less paper work, and the efficiency of operations, in general.

Smart Cities: The idea of smart cities is heavily dependent on the IoT-based infrastructures that handle the delivery of such services as transportation, energy distribution, waste management, and the security of the population. The combination of Blockchain and IoT can be used to develop safe, decentralized, and data-driven urban ecosystems [15].

The IoT gadgets that are installed throughout the city in a smart city based on blockchain capture information including air quality, traffic congestion and energy usage that is stored in the distributed ledgers to safeguard transparency and the authenticity of the data. This unchanging information may be utilized to create predictive analytics and automated functions in the city.

Indicatively, smart parking systems, which involve the use of Blockchain to locate and validate parking space occupancy, as well as payment processing by means of smart contracts, can be used to find unoccupied parking slots. On the same note, smart grids exploit the Blockchain to facilitate peer-to-peer (P2P) energy exchange between consumers and producers and ensure efficient and sustainable utilization of energy [15].

Removing centralized disorder lies will mean that Blockchain will allow the establishment of trust and auditability of data within different departments and services publics and areas that reached citizens and promoted openness in its management.

Energy and Internet of Energy (IoE): Energy industry has grown into distributed production and renewable infrastructures that result in the advent of the Internet of Energy (IoE) a decentralized form of energy management. The IoT blockchain technologies are essential to the energy trade, grid balancing, and optimization of resources [15].

With the IoT based smart meters, data on energy consumption and production are automatically retrieved and passed to the blockchain to be stored. Smart contracts support immediate acquisitions of energy between the producers (e.g. a household, equipped with solar panels) and consumers without involving third party intermediaries. This is a peer-to-peer trading model that increases the use of renewable energy sources by building transparency, lowering costs and encouraging their utilization.

The example of Brooklyn Microgrid and Power Ledger can be viewed as practical applications of the Blockchain-IoT where consumers are able to purchase and sell excess energy in a local market, which builds a trustless and transparent ecosystem of energy [15]. Additionally, Blockchain audit trails will guarantee proper billing, and they encourage the participants to behave in a sustainable manner with respect to energy use.

Industrial Automation and Industry 4.0: IoT gadgets find extensive applications in the domain of industrial automation, so-called Industry 4.0, as this type of information technology enables machine-to-machine (M2M) communication, predictive maintenance, and real-time analytics. But this centralization of the existing industrial control systems provides vulnerabilities of tampering of data, unauthorized access as well as resilience of single points

of failure. Incorporation of blockchain offers a decentralized network to ensure communication security, verify transactions and manage identities in industrial networks [16]. IoT systems are based on blockchain that allows automatic interaction between robots, sensors and manufacturing machines. Smart contracts can be used to give an example, to order raw materials or do a maintenance request automatically based on real-time sensor data. This will reduce downtime and human factor and enhance productivity and reliability.

In addition, Blockchain increases supply chain traceability in the manufacturing industry, which implies that all the parts utilized in the production procedure may be tracked to their origins avoiding counterfeiting and ensuring safety and adherence to regulatory requirements [14]. Consequently, the integration of Blockchain and IoT is an important indicator of the development of secure, resilient, and self-regulating industrial environments.

Agriculture and Food Security: Blockchain-IoT systems are also important in the field of agriculture and food supply control, associated with the transparency, safety and sustainability problems. IoT sensors used in farms monitor the moisture content of soil, temperature, and fertilizer application, and the data are stored in Blockchain to verify the information to be traceable and held accountable [14].

The use of the Blockchain-based applications enables consumers to calculate the origin of agriculture products, the conditions under which they are stored and transported. This provides safety of food and consumer confidence. Crop payments will also be automated through smart contracts, and payouts will be made on real-time sensor data which will reduce administrative delay and financial risk to the farmers.

Precision agriculture is therefore possible with the combination of the Blockchain and IoT, which facilitates the efficient utilization of resources, waste minimization and sustainable ecosystems of food.

Table 2: Comparative Overview of Key Applications.

Sector	Primary IoT Function	Blockchain Benefit	Example Implementation
Healthcare	Remote monitoring, EHRs	Data integrity, access control	MedRec, Chronicled
Supply Chain	Asset tracking, logistics	Traceability, anti-counterfeit	IBM Food Trust, VeChain
Smart Cities	Public data sensing	Transparency, automation	Smart Dubai, CityOS
Energy	Smart metering, P2P trading	Decentralized billing	Power Ledger, Brooklyn Microgrid
Industry 4.0	Automation, M2M	Security, process	Siemens Blockchain

	communication	optimization	Factory
Agriculture	Smart farming, IoT sensors	Provenance, sustainability	AgriDigital, TE-FOOD
Transportation	Fleet management, autonomous vehicles	Data sharing, safety	IOTA, MOBI Alliance

Transport and mobility systems: The transport industry enjoys the use of Blockchain-IoT as it provides vehicle tracking, autonomous mobility, and logistics optimization [16]. IoT sensors installed on connected vehicles will be able to note the driving statistics, health sensor statistics, and vehicle maintenance logs directly on Blockchain ledgers, which implies an untampered accounting system.

8. ISSUES AND FUTURE AREA OF RESEARCH

Although potentially demanding, Blockchain and IoT integration have technical and regulatory obstacles as well as scale challenges. The main impediments of large-scale deployment include high-energy consumption, interoperability, and latency [17]. Research planned in the future is on lightweight cryptography algorithms, quantum-resistant ones and how this can be combined with Artificial Intelligence (AI) to create adaptive IoT networks [18]. The legal frameworks and data governance standards should be changed to facilitate decentralized data ecosystems [19]. This section will examine the major areas that have revealed radical potential in IoT enabled by blockchain, which include healthcare, supply chains, smart cities, energy system, and automation in industries.

8.1 FUTURE SCOPE

The favourable development notwithstanding, there still are some technical and organizational solutions to consider until the integration of Blockchain and IoT is widely adopted. The further development of research and design is probably aimed at the following:

Scalability and Interoperability: The state of Blockchain frameworks are unable to support the colossal amount of transaction that IoT devices produce. The next direction of the work should be the scalable Blockchain architectures and cross-chain interoperability protocols allowing a smooth exchange of the data between heterogeneous networks.

Lightweight: Despite lightweight model advances, more creativity is needed to come up with ultra-low-energy consensus-based protocols that can be used by constrained devices in IoT, particularly in energy-sensitive services such as wearables healthcare systems and remote sensors.

The combination with the concepts of Artificial Intelligence (AI) and Edge Computing: The combination of AI, Blockchain, and IoT (which is often called AIoT) is a new trend that could improve predictive analytics, autonomous decisions and network optimization. The use of edge computing along with Blockchain will also decrease the latency and enhance the scalability of the system as the data will be processed near the source. **Standardization and Regulatory Frameworks:** Global standards do not exist in Blockchain-IoT systems and are a major challenge to interoperability and compliance. Governments, industries, and research entities should engage in collective actions to come up with standardized protocols and data governance structures of embedding the aspects of security and privacy.

Quantum-Resistant Cryptography: As a result of quantum technology, the concept of quantum computing has led to a risk of cryptographic algorithms becoming vulnerable. It is also important to develop quantum-resistant solutions of the Blockchain to maintain the long-term security of the IoT ecosystems.

Sustainability and Environmental: Impact Future Blockchain-IoT designs need to focus on sustainable computing models with limited energy usage, favored green technologies, and in line with the global sustainable objectives, including the Sustainable Development Goals (SDGs) of the United Nations.

9. CONCLUSION

The intersection of the IoT and the technology of Blockchain means the one of the most significant changes in the era of the digital transformation. IoT is linked with billions of heterogeneous devices that can sense, process, and transmit data and Blockchain brings in the concepts of decentralization, immutability, and trustless verification of networks. The combination of these creates one potent structure that improves the level of data integrity, transparency, and automation in a variety of applications, including healthcare and supply chains, smart cities and industrial automation [6], [11], [14].

By incorporating Blockchain and IoT, the two integration methods effectively overcome some of the major challenges being experienced by traditional systems of IoT including manipulation of data, the threat to privacy, and centralization vulnerability. With the help of smart contracts, devices can communicate with each other and they can perform specific conditions and deem needless human intervention. Also, the cryptographic and consensus schemes of Blockchain guarantee safe communication of information and avoid unauthorized accessibility of data and single points of failures.

Another point that was put forward in the chapter was that the choice of the Blockchain architecture between public, private, and consortium is tied to the level of decentralization, performance, and confidentiality, depending on the balance to be achieved [9], [10].

PoA and Pragmatic Byzantine Fault Tolerance (PBFT), Delegated Proof of Stake (DPoS), and DAG-based mechanisms were discovered to be the most promising solutions to the IoT networks because of their low latency, high throughput, and energy efficiency [11], [12]. These are lightweight and hybrid protocols that allow scaling and have network security, which makes them applicable to enterprise and public IoT ecosystems.

The practical applications also prove the revolutionary power of the implementation of the combination of Blockchain and IoT. Within the medical field, Blockchain protects patient records and boosts privacy; within the supply chain, it enables traceability and curbs counterfeiters; in the energy sector, it enables energy trading that is decentralized; and within automation of industries, it enables autonomous machine-to-machine communication [13] - [16]. All these applications highlight the increased topicality of Blockchain-IoT systems as the means of creating secure, transparent, and efficient digital systems.

10. REFERENCES

1. M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” IEEE/ACS Int. Conf. on Computer Systems and Applications, 2016.
2. L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
3. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.
4. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
5. Z. Zheng et al., “An overview of blockchain technology: Architecture, consensus, and future trends,” IEEE Int. Cong. on Big Data, 2017.
6. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
7. M. A. Salah et al., “Blockchain-based IoT identity management: A survey,” Security and Communication Networks, 2019.
8. V. Buterin, “A next-generation smart contract and decentralized application platform,” Ethereum White Paper, 2014.

9. H. Kim and M. Laskowski, “Toward an ontology-driven blockchain design for supply-chain provenance,” Intelligent Systems in Accounting, Finance and Management, 2018.
10. X. Xu et al., “A taxonomy of blockchain-based systems for architecture design,” IEEE Int. Conf. on Software Architecture, 2017.
11. A. Dorri, S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” IEEE Communications Surveys & Tutorials, 2019.
12. H. Li et al., “A hybrid consensus mechanism for blockchain-based IoT networks,” IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6192–6202, 2020.
13. M. Agbo et al., “Blockchain technology in healthcare: A systematic review,” Healthcare, vol. 7, no. 2, 2019.
14. K. Toyoda, P. Mathiopoulos, and I. Sasase, “A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain,” IEEE Access, 2017.
15. Y. Zhang and J. Wen, “The IoT electric business model: Using blockchain for the Internet of Energy,” Peer-to-Peer Networking and Applications, 2017.
16. M. Samaniego and R. Deters, “Using blockchain to push software-defined IoT components onto edge hosts,” IEEE Int. Conf. on Computer and Information Technology, 2016.
17. F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” Telematics and Informatics, 2019.
18. H. Kouicem, A. Bouabdallah, and H. Lakhlef, “Internet of Things security: A survey and taxonomy,” IEEE Communications Surveys & Tutorials, 2018.
19. M. Swan, “Blockchain: Blueprint for a new economy,” O'Reilly Media, 2015.