Chapter 3
Fusion of Blockchain and IoT: The Future of Industry 4.0

Ruchika Gupta, Shiv Ranjan, and Gagan Kukreja

3.1 Introduction

Industry 4.0 consists of the integration of manufacturing networks using cyber-physical structures, thereby allowing manufacturing facilities and development processes to transition into automated and complex networks. This autonomous system involves communication between the components of a "smart factory," both internally and with other factories that are built using IoT.

The number of attacks on IoT gadgets has greatly increased in recent years. The vast majority of these attacks attempt to assume responsibility for IoT gadgets with the goal of shaping their own botnet. Botnets are a gathering of PCs acting together to finish some specific assignment. A few botnets are devoted to dispatch only DDoS attacks on explicit administrations. A Distributed Denial of Service (DDoS) assault is an endeavor to make an online service inaccessible by overpowering it with traffic from different sources. Therefore, IoT gadgets that are not protected with appropriate username-password combinations can be effectively undermined and shaped into a botnet to dispatch attacks on different administrations. Examples of malware that misused this IoT vulnerability are listed below [1]:

- **Mirai**: There was a major DDoS attack directed at KrebsOnSecurity on September 20, 2016 that came from various areas across the globe. The malware that was responsible for this attack was the Mirai malware, whose source code was made

R. Gupta (✉) · S. Ranjan
Amity University, Greater Noida, Uttar Pradesh, India
e-mail: rgupta@gn.amity.edu; sranjan@gn.amity.edu

G. Kukreja
Ahlia University, Manama, Bahrain
e-mail: gkukreja@ahlia.edu.bh

T. Choudhury et al. (eds.), *Blockchain Applications in IoT Ecosystem*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-65691-1_3

publicly available by the pseudonym Anna Senpai. This same malware was used on October 21, 2016 to dispatch a massive reach attack on Dyn Domain Name Servers (DNS), which culminated in a large number of downtime pages. The working guideline of Mirai malware is as follows:

  - **CnC server:** A single Command-and-Control (CnC) system monitors all Mirai-infected computers and places them under its control. The ransomware emerges like a worm and attacks primarily IoT users. Once a device has been compromised, it waits for CnC server commands to start its attack.
  - **Loader:** The loader system distributes the malware to computers until it identifies a computer with the default username-password combination.
  - **IoT devices:** In the most operating concept, the malware seeks a series of default username-password combinations on every network. Because many IoT device users do not adjust their default username-password combination, they are very easy victims of the malware and quickly fall under the CnC server power.

- **Hajime:** Hajime is a Mirai variant that adopted the same operating concept as Mirai. However, its CnC service is not a single node but rather a distributed collection of peer-to-peer (P2P) servers that make it more challenging to take down. The hackers are still in active development.
- **IoTWorm:** A few analysts from Israel discovered another novel assault that could begin a chain response to make smart lights unusable and can disable a smart light system of an entire community. Such lights use an encryption key AES-CCM (Advanced Encryption Standard- Counter with CBC-MAC (Cipher Block Chaining, Message Authentication Code) to validate the reset of the firmware, so all lights use an AES-CCM equivalent switch. The AES (Advanced Encryption Standard) key can be acquired by a side channel test. Using powerlessness in the ZLL (Zigbee Light Link networks) convention's touch link component, the lights can be ejected from their specific controllers and malevolent software updates can be subsequently sent by labelling them with the AES key. When lights use the same AES key, heightening this attack exponentially and resolving any single smart light in a region is incredibly easy [1].

A potential solution to these problems is to use encrypted public-key networks for all interactions between IoT devices and Blockchain to ensure the security of the public-keys. Using a public-key dependent authentication system with a shared key infrastructure (PKI) would have prevented both the Mirai and Hajime attacks because it would have become more difficult to determine the private keys of many IoT users. The IoTWorm would also not have spread rapidly because separate IoT devices would have private individual keys and not a common key for all devices. To obtain the key and send out the malicious updates, each light would need to be hacked manually.

Moreover, with the advancement of 5G technology and future developments up to 8G technology, IoT has been growing rapidly and has been implemented by

almost 85% of companies. IoT endpoints are anticipated to expand at a compound yearly development pace of 32% from 2016 to 2021, reaching an introduced base of 25.1 billion units, as indicated by Gartner's forecast [2]. However, due to security and scalability issues, its benefits are unclear.

Therefore, it is imperative to understand what IoT is. What are the major concerns of users of IoT? How will we resolve these concerns? What is Blockchain? What are the challenges of the fusion of Blockchain with IoT? What is the future of the fusion of Blockchain with IoT? Will advanced features of IoT be developed to replace the benefits of Blockchain? This chapter describes one of the possible ways IoT and Blockchain technologies can be integrated to solve the given problems. The chapter also examines the feasibility of integrating Blockchain with IoT technology, prospective obstacles, and the advantages such convergences can bring.

3.2 IoT: Benefits and Challenges

IoT integrates humans, locations, and objects, rendering them 'smart' and able to interact with each other. IoT collects big data by continuously observing the real environment, processing, and taking a smart action centered on the same data. It makes the seamless convergence of the digital and physical realms feasible, thereby shifting the very meaning of our real-world experience [3].

Complex processors, cameras, and actuators are implanted into physical items, with each moving information to the IoT network. Thereafter, the analytical tools of IoT use this information to transform thoughts into training, impact advertising practices, and add creative methods of working. Thanks to the network of user-friendly devices, a person may access data irrespective of their role. Because communications are not fluent and transparent, inefficiencies are caused. However, in a network of interconnected devices, better connectivity is feasible because sending data packets over a wired network saves time and resources. Not only does IoT save time and money, it also encourages automation – the most critical aspect of today's tech-savvy existence, in which all tasks can be performed without human intervention with improved service quality [4].

The platform is gaining immense traction in the industry; as a result, it was projected that approximately 75.44 billion IoT-linked devices will be accessible worldwide by 2025 [5]. However, a variety of technological and health issues remain unaddressed. One of the issues with current IoT implementations is the need for a centralized entity (such as a cloud server) to communicate and interact through the Internet, which poses a major challenge to the privacy and security of the vast amounts of sensitive data that are produced. The original network concept requires a decentralized infrastructure, such as a peer-to-peer or distributed framework.

In contrast, the client-server model is very expensive in terms of high latency costs and low interoperability due to insufficient data exchange, device heterogeneity, coordination requirements with other distributed IoT networks, maintenance costs, and network equipment expenditures. The cloud service becomes a single

point of failure, thereby undermining the entire network and making resources ineffective when evading the scenario.

Security has become a significant IoT worry that has upset its enormous scope organization. IoT gadgets often experience the ill effects of security vulnerabilities, which make them an obvious target for attacks, including Distributed Denial of Service (DDoS). A few DDoS assaults have caused disturbances for associations and individuals lately. Unsecure IoT applications provide digital lawbreakers access to hack them into propelling DDoS assaults [3].

Another issue with current IoT frameworks is that of flexibility. As the amount of devices connected through an IoT network increases, current fused structures to validate, support, and interface different centers in a framework will become a bottleneck. This would require huge endeavors to create servers that can manage the colossal amount of information exchange, and the entire framework can go down if the server becomes difficult to reach.

While talking about the issue of IoT security, some rush to accuse the clients. Shoppers, they state, do not think enough about the associated gadgets they are introducing in their homes and working environments. They do not comprehend that the gadgets need refreshing, like personal computers and cell phones. Also, they overlook that the microwave or refrigerator is online and requires updates like some other devices. However, governments around the globe are endeavoring to manage this test of consumer mindfulness with regards to IoT security, progressively coordinating efforts and exhortation towards end clients.

In such a situation, with the end goal for IoT to succeed, highly coordinated activities are required across the board. IDC (International Data Corporation) had anticipated that practically 90% of associations using IoT will experience an IoT-based penetration of their back-end IT frameworks in the near future [6].

3.3 Blockchain Technology: Functions and Usefulness

On the most fundamental level, a Blockchain is an extraordinary sort of database wherein 'blocks' of successive and unchanging information related to physical/virtual resources are connected through cryptographic hashes, which are also appropriated as ever-developing 'chains' among numerous shared hubs. Blockchain increases are rendered after ratification by multiple hubs that use an arrangement method; the two simplest methods are Proof of Stake (PoS) and Proof of Work (PoW), upon which the new squares are allotted to all hubs. PoW is the most well-known negotiation instrument right now, with Bitcoin mining by solving cryptographic riddles being the most common concept. In any case, PoS requires lower processing assets and power, and it can convey quicker throughput.

Each personal computer (PC) in the network organization has its own network replication, which means that there are thousands, or a massive amount of duplicates of the corresponding Blockchain due to Bitcoin. Although Blockchain replication is identical, distributing the data through a computer network makes it extremely

challenging to monitor the data. For Blockchain, there is no singular, definitive record of controllable times. Alternatively, a programmer needs to monitor any Blockchain duplication on the network. Therefore, Blockchain is referred to as a "distributed database."

There are two types of Blockchain frameworks: permissionless (which anyone can join) and permissioned (in which individuals are confirmed by whoever is running the network). The latter can be further divided into 'private' and 'network' Blockchain frameworks – a lone endeavor versus associations connected by a particular business process, for example. In permissionless blockchains, such as those that underpin Bitcoin and Ethereum, consensus mechanisms are considered more reliant for affirming identities and verifying transactions [7].

As an appropriated record, Blockchain can be used to record any exchange, as well as monitor any advantage and related installments. Contrasted with conventional business forms, Blockchain can convey time and cost reserve funds, along with better security – particularly in a permissioned arrangement.

Operation of Blockchain The foundation for building a Blockchain is a P2P network that includes all the devices required to achieve the goals of the application. Asymmetric cryptography is used to assign two keys to each of the nodes: a public key to identify a machine on the network, and a private key to enable transactions on the network between themselves or other computers. When a device wants to make a transaction, it signs with its private key, transfers it to its neighbors for verification, and then disseminates it across the network. The private key offers confidentiality and integrity; miners bundle numerous such transactions into a block of timestamped transactions before they are verified by the network. Block validation may be achieved by several methods and then transmitted to the network, where all the nodes verify the block and its transactions, as well as the hash connection with the previous iteration. It is attached to and modified in the chain when tested, and otherwise discarded [6].

Blockchain uses four main concepts as its basis:

- **P2P network**: Eliminates the central Trusted Third Party and means that all network nodes have the same rights.
- **Accessible and distributed ledger**: A clear network where each node independently assesses the authenticity of a transaction.
- **Mining**: Network delays occur in a distributed system and not all nodes receive blocks of transactions at the same time. Therefore, any node must be prohibited from introducing a transaction to the chain, because the chain must have only one true and organized branch.
- **Synchronization of ledger copies**: Nodes come with a backup of the same ledger. The updating of ledgers by techniques is then used to transmit the new transactions to the network, validate the new transactions, and generally connect the authorized transactions to the ledgers [6].

Blockchain technology takes care of encryption and faith problems in many respects. Firstly, new blocks are still placed chronologically and linearly. Therefore,

they are still connected to the Blockchain's " top." When you glance at the ledger in Bitcoin, you will find that each block has a place on the list, labeled as a "height." As of January 2020, the height of the block had reached 615,400 [8].

After connecting a square at the edge of the record, it is extremely difficult to reach back and change the block's substance. Each square has its own hash, and a square hash before it. A mathematical formula makes hash codes and changes advanced data into a series of numbers and letters. In the event that the data are changed at a certain point, the hash code consistently moves.

Blockchain Usefulness Within the ledger, the 'blocks' store details on cash-related trades. However, for unexplained purposes, Blockchain is still a fully secure way of transmitting knowledge among different forms of exchanges. Blockchain software can be used to store property trading records, stops in a scalable chain, and even applicant-friendly decisions.

Deloitte interviewed 1000 organizations in seven nations on integrating Blockchain in their activities. Their research showed that 34% currently had a Blockchain implementation, while another 41% have plans to implement a Blockchain program over the next year. Likewise, approximately 40% of the organizations surveyed expected to invest at least $5 million in Blockchain in the coming year [3]. Blockchain has the potential to improve performance in the following areas:

- **Banks:** Buyers will have their transactions managed in as little as 10 min when integrating cryptocurrency into banks; this is basically the period it takes to connect a square to the network, with no restriction on the time of day or day of the week. Furthermore, through Blockchain, banks have the ability to exchange assets more easily and anonymously between organizations. Capgemini, a French consultancy, assessed that buyers may have saved $16 billion in banking and security charges in 1 year via Blockchain-based software [20].
- **Health care:** Medical care providers may use Blockchain to store the health data of their patients in a safe manner. This can be built into the Blockchain exactly where a health report is made and signed, which provides patients with verification and confidence that the document cannot be altered. Such unique accounts of success will be stored and managed with a private key on the internet, and they would only be reached through clear individuals, thereby ensuring security.
- **Voting:** Casting a Blockchain vote may prevent misrepresentation of the electoral judgment and boost voting participation. Each vote on the Blockchain can be placed away as a square, making it impossible to alter. The Blockchain conference will similarly make the administrative process clear, reducing the workers needed to direct a government judgment and providing quick outcomes to authorities.
- **Monitor supply chains:** When it comes to tracking supply chains, blockchain is extremely advantageous. By discarding the paper-based method, companies can easily identify unnecessary elements within their supply chains, even by

gradually discovering items. Therefore, Blockchain would enable companies, and probably even customers, to see how products are handled from a quality assurance point of view from their source to the store.

- **Copyright and eminence assurance:** Copyright and distribution laws for music and entertainment have been unclear in an environment of evolving Internet access. With blockchain, copyright laws for advanced material downloads will be greatly extended, ensuring that the craftsman or manufacturer of the substance being purchased earns a substantial amount of money. Blockchain can likewise provide performers and creators with constant and clear ownership knowledge.
- **Smart contracts.** On top of a ledger, smart contracts may be designed and work as decentralized applications. These programs may provide functions that are becoming increasingly complex as the need for traditional legal contracts fades.
- **Property.** Property titles, sales, and value can be assembled onto the Blockchain, providing clarity and decreasing the time and cost related to property transactions.

These are only a portion of the conceivable outcomes that accompany the new innovation. Currently, there are only murmurs in the business world of how Blockchain innovation can disturb the current models. Blockchain must be implemented with a goal to drive operational efficiencies. If appropriately executed, Blockchain innovation has even more extensive ramifications – without a doubt, positive ones.

3.4 How Can Blockchain Solve IoT Safety Issues and Scalability?

An IoT network can maange data transfers through numerous devices controlled and operated by different entities, making it impossible to determine the cause of any data breach in the event of a cyber-criminal attack. Furthermore, the IoT produces a large array of data, and the control of the data is not necessarily transparent for many parties involved.

Blockchain has the ability to help solve some of the issues surrounding IoT insurance and versatility. Blockchain, because of its unique features, is a technology game changer. It provides a method to gather clients to archive and trade the subtleties. Selected agents of this gathering hold their duplicate of the record and will commonly check every single new exchange through an agreement component until they are allowed onto the record [3].

Blockchain can help reduce the security and adaptability concerns related to IoT in the following manner:

- The flowed record in a Blockchain system is deliberately planned, which provides the necessity for trust among the included parties. No single affiliation has order over the enormous proportion of data generated by IoT devices.

- Utilizing Blockchain to store IoT data would incorporate another layer of security that software engineers would need to avoid in order to pick up induction to the framework. Blockchain provides a more robust level of encryption that makes it very difficult to overwrite existing data records.
- Blockchain engineering can decentralize the DNS, move the content to numerous hubs, and make it nonsensical to hackers. Modification rights should be provided only to the persons who require them (space owners) and no other user may make modifications, which significantly minimizes the possibility of accessing or altering knowledge by unauthorized people. A system can guarantee that it is resistant to programmers by using Blockchain to protect the details, even if each and every hub is cleaned off at the same time.
- When an exchange is started, approval of the information square is done through agreement between the system partners. At that point, the information is confirmed for all time, except if any approved changes are made to the information. At that point, it is encoded with the strongest encryption conventions to ensure information security.
- Smart contracts, a two-party agreement that is held in the Blockchain, can additionally permit the execution of legally binding understandings between parties, subject to certain conditions being met. For instance, when the prerequisites for the conveyance of assistance have been satisfied, smart contracts will support installments naturally, without the necessity for human intervention.

3.5 Feasibility Considerations for Integrating Blockchain and IoT Technologies

Blockchain addresses IoT issues by decentralizing the dynamic to an agreement-based shared system of devices. Be that as it may, when structuring the design for IoT devices related to a Blockchain record, there are a few plausibility issues to consider [3]:

1. The protection of exchange history in the mutual record for a system of IoT gadgets cannot be effectively allowed on an open Blockchain. That is because an exchange design investigation can be applied to make inductions about the personalities of clients or gadgets behind open keys. Affiliations should examine their security requirements to determine whether cross variety or private Blockchains may better suit their requirements.
2. One of the most important problems still facing IoT is one of scale: how to handle the vast volumes of data produced by a massive array of sensors. Defining a sensible data model in advance can save time and thwart difficulties when bringing the course of action into creation.
3. IoT devices have limited capabilities, and they lack virus and malware protection software, making them easy targets for hackers.
4. High exchange costs are likewise an inhibitor for collaboration.

5. Similarly, the resolute nature of IoT sensors may be undermined by interfering with the correct estimation of the measures that ought to be met to execute a trade. Measures should ensure the trustworthiness of IoT devices, with the ultimate objective that they cannot be changed by outside interventions; this ensures the protection of data recording and trades.

3.6 Examples and Use Cases of IoT Blockchain Technologies

There are numerous examples and use cases of IoT-enabled Blockchains, such as the following [3, 9, 10]:

1. **Smart appliances:** A smart appliance is a web-enabled device that offers additional data and power compared with traditional appliances. For example, when your medications are scheduled or your laundry cycle has ended, a code linked to your device can be attached to the web and alert you. Such alerts keep your devices in perfect order, save the user money in terms of productivity output, and allow the user to monitor their equipment while away from home, among other benefits. Encoding these Blockchain devices guarantees your ownership and allows transferability.
2. Helium**:** Helium is the world's first decentralized network of machines. The organization uses Blockchain to associate low-control IoT machines (e.g., switches, microchips) to the Web. Helium's Blockchain-based remote web foundation uses radio innovations to fortify web associations and radically decrease the resources needed to operate smart machines.
3. **Supply chain sensors:** Sensors include items of measurable consistency in the supply chain to collect data on the region and state of the structures when they are sent for distribution. In a 2016 survey of 900 leading supply chain companies, Deloitte and MHI Research discovered that 44% of respondents used sensors, with 87 percent planning to use the technology by 2020. These advancements would results in up to 1 trillion sensors by 2022 and up to 10 trillion sensors by 2030. The Blockchain holds the data, then controls, guarantees, and transfers it [21].
4. **Riddle & Code:** It integrates smart card authentication by incorporating blockchain technologies with cryptography to establish a hardware-based digital identity for all physical objects connected together. These connected objects communicate securely using highly secured crypto chip which enables them to become individual blockchain node. Communication and transactions between devices are autonomously and securely performed using a highly secure crypto chip made up of an adhesive nonremovable tag which enables each device to become a blockchain node. In addition, an Android program is used to perform a blockchain transaction in order to register the chip's special, tamper-proof identity. It will communicate with other devices once it has been tested in the network.

5. ArcTouch**:** This service creates and fabricates Blockchain-based programming for a scope of smart, associated things, including voice aides, wearable devices, and smart televisions. The service has assembled customized, decentralized apps (DApps) for many organizations that connect to IoT gadgets. ArcTouch's DApps provide an additional degree of IoT security and can process requests quicker through smart agreements. The organization has assembled a few Blockchain DApps that can be associated with IoT gadgets, such as Amazon Alexa.
6. **Modum.io:** This service solidifies IoT sensors with Blockchain advancements, providing data integrity to trades, including physical items. The sensors record normal conditions, such as temperature, that product is reliant upon while in movement. When the product appears at a transit point or end customer, the sensor data is verified against fated conditions in a smart agreement on the Blockchain. The agreement ensures that the conditions meet all requirements set out by the sender, their clients, or a controller and triggers various actions, such as notifications to the sender and beneficiary, amount, or appearance of product.
7. HYPR**:** This service utilizes decentralized systems for associated ATMs, vehicles, and homes. One of the fundamental reasons cyberattacks are so obliterating and across the board is that unified databases store a huge number of passwords. HYPR stores biometric logins on its Blockchain, verifying and decentralizing significant data. The organization's biometric security conventions incorporate remarkable facial, eye, voice, and palm recognition instruments for IoT gadgets.

3.7 Benefits of Integrating Advanced IoT for Blockchain Networks

Blockchain enables IoT gadgets to upgrade security and acquire straightforwardness in IoT systems. As indicated by IDC, 20% of all IoT arrangements were using Blockchain-based arrangements by 2019. Banks and financial institutions, such as HSBC, are using PoC to affirm the Blockchain development. In addition to financial establishments, a wide range of associations are using the capacity of the Blockchain [6].

IoT provides boundless open entryways for associations to run smart assignments. Many devices are equipped with sensors, sending data to the cloud. Thus, consolidating the two innovations of IoT and Blockchain can make the frameworks more productive. Some advantages offered by this coordination are as follows:

- Increased security and trust in shared multi-party exchanges and information
- Increased business proficiency and reduced expenses.
- Increased income and business opportunities
- Improved constituent or member experiences

However, the advantages provided by this combination vary by industry. Some of the advantages associated with this reconciliation from various ventures are described in the following sections [11].

Logistics and Supply Chain A worldwide supply chain includes numerous partners, such as specialists and crude material suppliers. Additionally, the supply chain can extend over long stretches of time and comprise a huge number of installments and solicitations. Because of the contribution of different partners, conveyance delays become the greatest test. In this way, organizations are attempting to make the vehicles IoT-empowered to follow the development all throughout the shipment process. Because of the absence of transparency and intricacies in the current supply chain and logistics, a Blockchain and IoT combination can help to upgrade the quality and discernibility of the system [12].

Both the organization and the purchaser can follow the item's entire life cycle throughout the supply chain utilizing Blockchain and IoT features. Blockchain is a complete information record where all the interchanges among IoT gadgets are captured in the history. It gives instant access to all data associated with the items, such as the dates a fish was harvested, processed, and sold – a total record of its excursion from sea to fork. Once information is saved on the Blockchain, collaborators that have signed Agreements eventually obtain access to the details. Supply chain members can similarly prepare for shipment and run cross-border exchanges.

Construction Industry The construction process includes many experts who need to exchange data to configure and actualize projects effectively. There are many intermediaries who are used to verify the entire procedure, such as controllers, investors, backup options, legal advisors, and so on. There is a need to build trust among all the partners. The progress of tasks from conventional strategies to advanced structures is suited for a computerized approach, such as Blockchain, which can encourage and empower trust among players. For the individuals who need open, reliable IoT correspondences without depending on go-betweens, a private Blockchain could provide the arrangement and empower information security between IoT gadgets.

Blockchain additionally makes a dependable chain of events, exchanges, resources, and basic project details. This permits messages, project management frameworks, and bookkeeping frameworks to meet up in one spot, creating a validated record of all exchanges on the Blockchain and guaranteeing that information cannot be lost. It ensures that with each project, there is a single mutual adaptation of fact, and this is what the organization wants to prevent replication, minimize errors, and maintain data integrity. Some of the advantages it can offer include the following: Improve the transparency and trustworthiness of construction logbooks, works completed, and material supplies reported, providing a consistent infrastructure for information management at all phases of the building life cycle [13].

Automotive Industry Today's vehicles are advancing to be much more than just a transportation tool. The cars of the twenty-first century are moving server farms with local sensors and computers that collect vehicle information. With progressively stable, identifiable transfers and improved data access and integrity, Blockchain may reinforce trust and unify efforts between organizations, consumers, and even vehicles. The automotive sector is a fascinating use of IoT with Blockchain, in which centralized engineering interacts with computerized fuel deployment, self-sufficient cars, smart departures, and mechanized traffic management.

Blockchain innovations have assisted with the assembling of self-governing vehicles. Smart vehicles are outfitted with autopilot modes, which permit the vehicle to independently depart or perform different undertakings by training the vehicle's advanced computer utilizing voice commands. Because of the RFID labels on Blockchain-produced vehicle parts, every segment can be easily confirmed for credibility. The blockchain platform offers the highest degree of confidentiality and speeds up the vehicle ownership process. Blockchain additionally uses a smart contract, in which the dealer and purchaser can exchange merchandise without the requirement for a broker. Blockchain likewise triggers machine-to-machine (M2M) exchanges with the use of smart contracts [14].

Pharmacy Industry Blockchain-coordinated IoT can accelerate the pace and reliability of clinical trials and improve pharmaceutical supply chains. Additionally, as one survey from BIS Research showed, healthcare companies worldwide lose approximately $200 billion annually because of counterfeit or contaminated medications [15]. The transparent nature of Blockchain allows the distribution of medications to be monitored from manufacturing to shipment.

Agriculture From ranchers to makers and merchants, Blockchain combined with IoT is reinventing the food manufacturing industry. Blockchain can improve agricultural management practices using a simpler approach to maximize farming services such as water, labor, and fertilizers.

In IoT-empowered smart agriculture, the crop field is monitored with sensors for measurements such as temperature, pH, soil dampness, moistness, and light. IoT sensors and gadgets capture information that can assist farmers with making educated choices in the development of the crops. Artificial intelligence (AI) is applied to the information captured from the sensors to provide valuable bits of knowledge with respect to crop identification and crop yield forecast, among others [16].

The high-quality information assembled by applying AI is stored in an interplanetary file system, an appropriated stockpiling stage where addresses are hashed and put away on the Blockchain. The data captured in the Blockchain trigger smart agreements to process rules characterized inside them. Smart contracts encourage the trading of information stored on the Blockchain inside particular partners in the framework. Because data are available to each agricultural business member, they will be able to effectively produce crops or food.

3.8 Prospective Barriers to the Convergence of Blockchain and IoT

The combination of Blockchain with IoT is not simple. Blockchain was intended for an online environment with powerful PCs, and this is a long way from the IoT reality. Blockchain exchanges are carefully marked; thus, devices suitable for working with cash must be equipped with this ability. Fusing Blockchain into the IoT requires further testing. The following are some of the recognized difficulties:

- **Certification security:** Given the way that Blockchain is recognized for its high-security standards, a network built on Blockchain is equally as safe as the direction of the application. Other authentication protocols, such as TLS (Transport Layer Security), are currently used by IoT application protocols to provide safe communications. Such reliable protocols are complicated and resource-intensive, and they necessitate centralized maintenance and governance of key infrastructure, which is usually accomplished by Private Key [17]. Also in such a scenario, loss of a record's private keys can provoke absolute loss of advantages, or data, obliged by this record. Therefore, this needs to be reviewed further.
- **Capacity limits and versatility:** As discussed, stockpiling limits and the adaptability of Blockchain are still under investigation. However, with regard to IoT applications, the inalienable limit and adaptability constraints make these difficulties a lot more noteworthy. In this sense, Blockchain may give off an impression of being incompatible with IoT applications, but there are methods by which these impediments can be mitigated or avoided. In the IoT, where gadgets can produce gigabytes of information progressively, this constraint is an incredible hindrance in its combination with Blockchain. Some current Blockchain executions can easily process several trades per second, so this could be a potential bottleneck for the IoT. Moreover, Blockchain is not intended to store a lot of information like those created in the IoT. A reconciliation of these advancements should manage these difficulties.
- **Processing Speed:** Concerns have been raised about the computing power needed to encrypt all of the objects in a blockchain-based ecosystem. The IoT networks, unlike traditional computer networks, are very complex and made up of computers with a wide range of computing capacities, and not all of them would be able to execute the same encryption algorithms at the same speed.
- **Unwavering quality:** Blockchain may be a key development to provide important security improvements in the IoT. One of the essential challenges in the combination of the IoT with Blockchain is the steadfast nature of the data generated by the IoT. Blockchain should ensure the data in the chain is unchanging and that it can recognise updates, regardless of whether data is somewhat compromised in the blockchain.

3.9 Conclusion

We are at the beginning of another period of Industry 4.0. The advancements in sensors and smart chips is growing rapidly, making them dynamically minimal and appropriate for a continuing relationship with Blockchain records. The blend of Blockchain and IoT has vast potential for the creation of a business focal point of organizations among devices, as well as providing organizations with the ability to create a driving force from accumulated data [18, 19]. The increase in Blockchain shows, affiliations, and IoT device providers demonstrates that there is a place for Blockchain in the IoT division.

To achieve an ideal, secure model of IoT, security must be included in the foundation of the IoT's natural framework, with intensive authenticity checks, approval, and data validation. All data must be encoded at all levels. Without a solid foundation, more risks will be created with every device added to the IoT. A protected and safe IoT with guaranteed security is needed. If we can overcome the disadvantages of Blockchain technology, it is an outrageous trade-off. It's important to note the Blockchain isn't a guarantee of stable IoT. Its suitability is determined by the way it is applied.

References

1. A. Kumar, T.J. Lim, A secure contained testbed for analyzing IoT botnets. https://arxiv.org/pdf/1906.07175.pdf
2. M. Arnott, P. Middleton, K. Sharpington, Internet of Things forecast database. Gartner Research, 05 November 2019
3. Driving Into Digital: Journey to the future, Deloitte. https://www2.deloitte.com/in/en.html
4. S.A. Wright, Privacy in IoT Blockchains: With big data comes big responsibility, in *IEEE Int'l Workshop on IoT Big Data and Blockchain (IoTBB'2019)*
5. Internet of Things (IOT) Connected Devices installed base worldwide from 2018 to 2025 (in Billions), Statista Research Department, May 2020. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/
6. R. Thakur, R. Vaghasiya, C. Patel, N. Doshi, Blockchain based IoT – A survey. Proc. Comput. Sci. **155**, 704–709 (2019) https://www.sciencedirect.com/science/article/pii/S1877050919310178
7. T.K. Sharma, Permissioned and permission less Blockchain – A comprehensive guide, Blockchain Council, Insights and Resources, November 2019. https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/
8. A. Chatterjee, What is bitcoin and Blockchain? Learn Blockchain and bitcoin quickly. Techtravelhub, May 2020. https://www.techtravelhub.com/blockchain/
9. Blockchain Infographics: Blockgeeks. https://blockgeeks.com/blockchain-infographics/
10. Blockchain: What is Blockchain technology? How does Blockchain work? Built-in Report. https://builtin.com/blockchain
11. IBM Blockchain is changing business, industries- and even the world, IBM Cloud Forum 2020. https://www.ibm.com/in-en/cloud/blockchain-platform/developer
12. Oracle Report: Blockchain in manufacturing – Answering the Clarion call for better traceability, January 2018

13. T. Ziga, Klinc Robert: potentials of Blockchain technology for construction management. Proc. Eng. **196**, 638–645 (2017)
14. Deloitte Report: Accelerating technology disruption in the Automotive Market. https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/consumer-business/deloitte-cn-consumer-blockchain-in-the-automotive-industry-en-180809.pdf
15. BIS Research: Global Blockchain in healthcare market 2018. https://bisresearch.com/industry-report/global-blockchain-in-healthcare-market-2025.html
16. Leewayhertz Report: Blockchain in agriculture-improving agricultural techniques. https://www.leewayhertz.com/blockchain-in-agriculture/
17. G. Chandra, R. Gupta, N. Agarwal, Role of artificial intelligence in transforming the justice delivery system in COVID 19 pandemic. Int. J. Emerg. Technol. Learn. **11**(3), 344–350 (2020)
18. P. Srivastava et al., Fuzzy methodology approach for prioritizing maintenance 4.0 attributes, in *2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, (IEEE, Dubai, 2020), pp. 308–311. https://doi.org/10.1109/ICCAKM46823.2020.9051483
19. A. Gupta, A.O. Salau, P. Chaturvedi, S.A. Akinola, N.I. Nwulu, Artificial neural networks: Its techniques and applications to forecasting, in *IEEE International Conference on Automation, Computational and Technology Management (ICACTM)*, (IEEE, London, 2019), pp. 320–324. https://doi.org/10.1109/ICACTM.2019.8776701
20. Smart Contracts in Financial Services: Getting from Hype to Reality, Capegemini Report, 2016. https://www.capgemini.com/news/consumers-set-to-save-up-to-sixteen-billion-dollars-on-banking-and-insurance-fees-thanks-to/
21. Accelerating change: How innovation is driving digital, always-on supply chains, The 2016 MHI Annual Industry Report, http://cpbucket.fiu.edu/1168-geb6368x81168_emba-97075%2F2016-industry-report-2016-(1).pdf