Chapter 7
Blockchain Mechanisms as Security-Enabler for Industrial IoT Applications

J. Rian Leevinson, V. Vijayaraghavan and Muthu Dammodaran

Abstract The introduction and enactment of Industrial Internet of Things (IIoT) have initiated a global revolution. The volume and variety of data that are collected and processed in industries are ever increasing due to the widespread acceptance of modern technologies such as Internet of Things (IoT), big data analytics, machine-to-machine (M2M) communication, edge computing, and cloud storage. Conventional systems with centralized architecture are not designed to handle the complexity and scale of data that is processed in IIoT operations. Moreover, the threat of security and privacy breaches also increases with the growth of IIoT-connected devices. IoT devices often tend to have poor security defense systems due to low processing power, limited storage capabilities, and poor manufacturing standards. In this context, blockchain technology can help to eliminate the security vulnerabilities faced by the IIoT systems and provides extensive protection from data thefts, cyberattacks, and data corruption. Blockchain with its distributed architecture offers peer-to-peer networking and enables auditable and transparent transactions. This chapter explores the concept of IIoT and its limitations, and the need for deploying blockchain mechanisms in the IIoT paradigm. We further analyze blockchain technology and how it can reinforce IIoT systems. Existing systems of blockchain in the IIoT ecosystems and relevant use cases are also explored. As conventional systems struggle to handle the scale of data operations handled by the IIoT, blockchain has emerged as a viable solution to reinforce and reform existing systems.

Keywords IIoT · I4.0 · Industry 4.0 · Blockchain · Cybersecurity · Supply chain · Data privacy · Cryptography

J. Rian Leevinson
Infosys Limited, Chennai, India
e-mail: rian.leevinson@infosys.com

V. Vijayaraghavan (✉) · M. Dammodaran
Infosys Limited, Bangalore, India
e-mail: Vijayaraghavan_V01@infosys.com

M. Dammodaran
e-mail: dammodaran.muthu@infosys.com

Z. Mahmood (ed.), *The Internet of Things in the Industrial Sector*, Computer Communications and Networks, https://doi.org/10.1007/978-3-030-24892-5_7

7.1 Introduction

The Industrial Internet of Things (IIoT), also known as Industry 4.0 or I4.0, refers to the extension and use of the Internet of things (IoT) in the industrial sector to build interconnected ecosystems. IIoT is used to integrate various machines, systems, actuators, and devices using sensors and IoT gateways so that they can seamlessly collect, process, and exchange data between each other. The introduction of IIoT and its subsequent implementation in the industrial world has completely changed how factories manage their systems and processes. IIoT is also one of the critical factors that drive Industry 4.0 which is considered as the current industrial revolution. This new generation of industries has integrated systems with a centralized architecture where all the systems are interconnected with IIoT. Data is collected using various sensors and it is transmitted to the cloud-based systems where they are stored, processed, and analyzed.

However, the swarm of interconnected devices generate massive volumes of complex data that conventional centralized systems struggle to handle. Security threats and vulnerabilities also tend to increase with the increase in the number of connected devices. Since more and more data is collected, privacy becomes another concern as any breach can compromise confidential information.

Blockchain, being a system of linked records, helps to overcome most of the limitations faced by the IIoT. Since blockchain is resistant to modifications and changes with sophisticated cryptography, it is considered extremely secure. The distributed system is also essential in industries and factories as even if one node fails, the rest of system must continue to function. This is not the case in conventional systems where the failure of the central system can cripple the entire network. Since the blocks in blockchain are secure by design, they offer excellent privacy and safety features. Combined with the IIoT vision, blockchain delivers unparalleled solutions that can empower and revolutionize industrial processes.

The flow of this chapter progresses as follows: Sect. 7.2 introduces the concept of the IoT and the issues faced by current IIoT systems as well as their subsequent impact. Section 7.3 analyzes blockchain technology, explores its features, and explains how blockchain helps to secure IIoT. Section 7.4 explores the architecture of a blockchain-IIoT platform in detail and provides a brief overview of popular blockchain platforms. Section 7.5 explores a few use cases of blockchain in IIoT. The conclusion is presented in Sect. 7.6.

7.2 The Industrial Internet of Things (IIoT)

The Industrial Internet of Things (IIoT) refers to the implementation of the IoT in the industrial sectors by integrating and interconnecting various machines and devices. The machines are embedded with electronic sensors, actuators, and other digital devices to collect, process, and store data. IIoT allows efficient and seamless

transmission of data between devices. The implementation of IIoT has led to smart factories, optimized production lines, smart environments, customized manufacturing, and increase in overall efficiency. The widespread acceptance of IIoT-related technologies is one of the major contributing factors to Industry 4.0 which is considered the fourth industrial revolution. This marks a new era in the industrial world which is led by IIoT, cloud computing, big data, and advanced analytics [1].

IIoT technology has been implemented in industries for a variety of uses such as the predictive maintenance, asset tracking, fleet management, warehousing, customized manufacturing, and efficient production lines. It has been used over a wide range of industries such as automobile, logistics, transportation, e-commerce, manufacturing, mining, and shipping [2].

Although IIoT sees widespread usage in the industrial sector, it suffers a variety of critical issues that are similar to those experienced by IoT-based systems. These shortcomings are mainly related to the security aspects, privacy, trust, and interoperability. These issues act as major hindrance toward the full-scale realization and implementation of IIoT technology in industries. Therefore, it is essential that these issues are well understood and appropriate solutions are proposed.

7.2.1 Issues and Limitations of IIoT

The lack of robust security architecture in IIoT networks renders them susceptible to cyberattacks [3]. This lack of security can be attributed to poor manufacturing standards, lack of interoperability, limited processing capabilities, and small storage capacity. Since industries involve confidential data like the design of new products, assembly procedures, financial, and personal data, an attack proof security model is essential [4]. Moreover, the data is most vulnerable when it is being transferred and IIoT systems lack strong encryption layers due to constrains in computational capabilities.

Privacy is also a major challenge in the IIoT paradigm. Protecting the privacy of the stakeholders by securing the data is essential. Privacy concerns arise primarily due to insufficient security measures in IIoT devices. Data is often transmitted with little or no encryption and can hence be easily misused by anyone who manages to access it. The large number of connected devices also poses a massive challenge to privacy as it is difficult to monitor the integrity and security of all the devices continuously. Moreover, since the devices are placed in remote locations at field sites in industries, they are vulnerable to data leakages and eavesdropping. IIoT devices need privacy by design to cope with global standards and increase adoption rates in industries [5].

System safety and reliability are the highest priority of many OT (Operational Technology) platforms. This means preventing the system and its components from causing unacceptable risk of injury or physical damage, protecting the environment against harm, and avoiding interruption of safety-critical processes. As most OT systems in the past were not networked, security and privacy were not a major concern. With IoT being extensively accepted and implemented, it is fundamentally

transforming this perspective in the industrial world. Networks of IoT devices are used to digitalize conventional OT systems. With the current connection of OT and IT (Information Technology) under IoT, remote attackers exploit the weaknesses in industrial, consumer, and public sector IoT systems to break into the OT system and drive it into an unsafe or unreliable state.

In addition, the employment of remote management that includes reconfiguration and updating of devices as well as monitoring and operational reprogramming is creating serious next-generation security and safety concerns. The introduction of IoT systems with open ports and the potential interjection of malicious code, especially on safety devices and systems such as transport, city public safety, and water are creating new requirements for security and safety that are not currently addressed appropriately.

IIoT systems face issues in integration and interpolation with existing operational systems. These mainly stem from the fact that conventional mechanical and operational systems lack the flexibility to accommodate new additions such as IIoT-based solutions. Moreover, the lack of manufacturing protocols and guidelines has led to the production of IIoT devices that are not interoperable with each other. This remains a key factor in the slow adoption rates of IIoT-based solutions in industries.

IIoT devices are often placed in inaccessible remote locations in industries that render conventional regular maintenance services impractical. This makes reliability a key factor in IIoT systems. Another issue with the placement of IIoT devices in remote locations is the problem of connectivity. IIoT networks may also face communication disruptions and interferences due to their close operational proximity to heavy machines. These disruptions and disconnections could lead to the loss of critical information and may cause system vulnerabilities.

7.2.2 Impact of Attacks on the IIoT

As modern organizations use IIoT networks to run their processes, they are exposed to a variety of security threats including data leakages, cyberattacks, data theft, dangers related with IT/OT assembly, and insider threats. IIoT ecosystems are especially prone to such attacks due to their poor security standards. If the vulnerability of the network is exploited, potentially catastrophic consequences like theft of critical data, loss of production, crippling the system, and data loss may occur [6].

Conventional mechanical systems store data in physical form or in local storages that provide a considerable amount of security. However, modern systems have huge volumes of sensitive data stored and transmitted online that makes them extremely vulnerable to security threats.

Modern IIoT networks are exposed to a variety of threats and the number of security breaches and exploitations is continuously on the rise. The main types of attacks include brute force attacks, hacked devices and networks, viruses, malware, worms, physical tampering, system assaults, and encryption attacks.

In the recent past, there have been successful attacks on extremely sensitive systems such as atomic power plants, water supply plants, and vehicles. Moreover, investigations have revealed critical vulnerabilities in existing IIoT applications such as medical pacemakers and cars. If such vulnerabilities are exploited, they could have dire consequences and can severely hamper the adoption of IIoT systems across industries.

7.3 Blockchain

Blockchain is a distributed transaction ledger that is used to maintain records of transactions and operations. It is a linked chain of blocks that contain the details about the transactions. When a new transaction is performed, a block is created with all the relevant transaction details and then connected with the other blocks. It essentially forms a distributed system that has a high level of interconnection between the transaction blocks unlike conventional blocks that have a central hub-based design.

Since blockchains are distributed and decentralized, exchanges and transactions in blockchain systems can happen without the verification of the central server. Thus, blockchain can altogether reduce server costs (counting the cost of optimization and operation) and alleviate the execution bottlenecks at the focal server [7].

Tampering data in a blockchain network is extremely difficult due to the fact that the blocks are connected with each other and the entire set of blocks has to be altered to change the data in any one block. Moreover, each communication block would be approved by different hubs and exchanges would be checked. In this way, any distortion in the network can be identified effectively [8].

Blockchain allows users to assume a considerable level of anonymity. Transactions are recorded and monitored and their location is registered but the identity of the individual is preserved. Moreover, the user can create multiple identities to evade detection as well. Such a level of anonymity is possible due to the distributed nature of blockchain networks although it is possible to determine the identity of the user by observing network traffic and the public blockchain system [9].

Since all the exchanges performed in blockchain networks are approved and recorded with a timestamp, clients can easily check and verify the integrity of past records by getting to any hub in the respective system. In Bitcoin blockchain, every exchange can be followed to past exchanges iteratively. It enhances the transparency of the information stored in the blockchain and makes it easily verifiable.

7.3.1 Salient Features of Blockchain

Blockchains are fundamentally different from conventional transaction networks and they have a variety of special features. Their key functionalities include cryptographic

encryption (asymmetric cryptography), hashing, linked blocks, and smart contracts. Due to their distributed nature, nodes can communicate with each other directly without being processed through a central server. This considerably reduces the time taken to process transactions and also improves the reliability of the platform. The system can continue to function even if a few nodes fail. This is not the case in conventional systems where the failure of the central hub can disrupt the entire network.

Direct encrypted transactions enforce privacy and considerably increase the security aspects of the system. Moreover, blockchains possess the advantage of being easily auditable and hence all the historic transactions can be checked and verified [10].

Cryptographic Hash Functions

Cryptographic hash functions are used in blockchain to mask and secure the data transferred in transactions. Hashing essentially standardizes the data by taking in various outputs, passing them through a mathematical function and giving output in a fixed format. It produces a unique hash value for each input and hence the original data can be easily retrieved. However, it is impossible to infer the input value from only the hash value and is thereby essential in securing the original data.

Hashing functions do not modify the original message and hence there is no data loss. Furthermore, hashing is entirely different even if there is a small alteration in the input. Hashing is an essential component of any blockchain security system and is extensively used in Bitcoin. Hashing is also used to check for integrity of the data [11].

Blockchain Transactions

A transaction represents an interaction between two parties. In the case of cryptocurrencies, transactions represent transfer of cryptocurrency between blockchain users. These transactions could also refer to the transfer of messages or recording activities [12].

Each block in a blockchain can contain zero or more transactions. For some blockchain implementations, a constant supply of new blocks (even with zero transactions) is critical to maintain the security of the blockchain network; by having a constant supply of new blocks being published, it prevents malicious users from decoding the blockchain and altering the blockchain itself.

Asymmetric Key Cryptography

Asymmetric key cryptography (public key cryptography) involves the usage of two distinct keys to encode the data. The original message is encrypted using the public key which is openly available to anyone. However, the data can be deciphered only using a private key which is securely shared among the stakeholders.

Asymmetric key cryptography is an essential part of blockchain cybersecurity. It is a key factor in ensuring the integrity of the messages transmitted through the blockchain system and securing various transactions performed through the system

[13]. Moreover, digital signals are used to verify the authenticity of transactions to ensure that the owner of the private key is the one performing the transactions [14].

Since modern IIoT systems tend to have thousands of devices connected together and communicating with each other, conventional cryptographic techniques are not capable of handling them. This establishes the need for advanced blockchain-based public key encryption techniques especially while handling high volumes of client–server interactions [15].

Blockchain Addresses and their Derivation

Blockchain systems utilize the concept of addresses as placeholders to enable transactions between entities. An address acts like a unique and secure identifier that is used to label and record transactions. Blockchain addresses are created by pushing the public key through cryptographic algorithms. The address essentially adds a checksum to the pubic key to prevent wrong transactions especially due to typing errors [16].

The addresses are usually generated using ECDSA cryptographic algorithm which enables the user to sign transactions with a private key and verify it using a public key. ECDSA ensures that the authenticity of the user is preserved by letting other users verify the author of the transactions. However, the public key is very long and inconvenient to use. Hence, the address is derived from the public key and is used to perform transactions.

Blocks in the Blockchain

Blockchain systems are essentially made of a series of blocks that are connected with each other. These blocks are an integral part of the blockchain system as they are the main entities which perform transactions and store relevant data.

Exchanges are added to the blockchain when a distributing hub distributes a block. These blocks contain data that is cryptographically hashed and also contain information about the previous block that enables the connection between them. This system can be used to assess and verify the integrity of the blockchain system by tracing the previous block connections back to the source block. These blocks also enable peer-to-peer data networking and data transmission as there is no centralized block and the system is distributed.

Legitimacy and credibility are guaranteed by ensuring that the exchange is accurately organized and that the exchanges have been cryptographically marked. Hence, the private key is used to decipher the messages received by a block; and the other full hubs will check the legitimacy and credibility of all exchanges in a distributed block [17].

Smart Contracts

Smart contracts are modern promises/contracts that are coded in a digital form and are governed by a set of rules. In blockchain, smart contracts act as decentralized applications that facilitate the implementation of complex algorithms. These contracts are generally governed by preset logics and mathematical functions to ensure automation of contracts between users [18].

A smart contract is activated by performing an exchange that invokes it. It executes autonomously and consequently in a desirable way on each hub in the system, as per the information that was incorporated into the exchange. They allow transactions to be performed directly and eliminate the involvement of third parties. Smart Contracts can be traced and audited but they are irreversible as making changes in the blockchain is very difficult [19].

7.3.2 How Blockchain Secures IIoT

Blockchain when integrated with an IIoT ecosystem increases the security prospects of the entire system. Blockchain has excellent privacy and security characteristics that are essential in IIoT systems. It is distributed, sealed, repetitive, and secure and thus helps IIoT systems overcome their critical drawbacks. Since blockchains consist of blocks of data that are interconnected and distributed, they are faster and more resilient to attacks as the data is not stored in a central hub; it is spread throughout the network. Besides, blockchains also use strong encryption algorithms and hashing techniques and are hence extremely secure. Blockchain transactions are also transparent and the identity of the users can be easily verified. This prevents malicious users and devices from penetrating and contaminating the blockchain network.

In IIoT environments, large portion of the correspondence is machine-to-machine (M2M) cooperation, with no human mediation at all. In such situations, setting up trust among the partaking machines is a major test that IIoT still has not met broadly. Blockchain improves trust among devices by ensuring the authenticity of the devices and offering extensive cyber protection. Such networks can also proactively detect [20].

Blockchain networks are tamper proof and extremely difficult to alter. This is essential in the case of IIoT devices as any attempt to manipulate or alter the sensor or gadget can be immediately identified and necessary proactive action taken [21]. If the integrity of any device is compromised, it can be safely and swiftly disconnected from the network as blockchain systems have a distributed design. They do not have dependency on any specific node in the network.

A circulated arrangement of record for sharing information over a distributed system enables fast transactions and thus making it almost impossible for the network to shut down as the failure of any one node will have minimal effect on the overall system. Hash-based securities, check of character, and provenance verification are essential in identifying rogue devices and alleviating dangers.

By enabling registration and validation of devices to enroll against the system, blockchain-coordinated IIoT arrangement can enhance the overall framework well-being. Smart contracts also encourage programmed execution of business rationale. In the absence of a focal framework to assault, dangers of system failure due to potential attacks on the central node can be avoided altogether [22].

7.4 Platform Architecture for Blockchain in IIoT

In this section, we explore blockchain platform for Industrial Internet of Things (BPIIoT) as proposed by Bahga et al. [23]. The BPIIoT uses distributed architecture, peer to peer network, and secure connectivity for usage in the industrial sector. This network is based on smart contracts that act as agreements between the customers and the manufacturers. These smart contracts are transmitted through the blockchain system and are essential in building trust among the stakeholders. The blockchain platform integrates the shop floor with the cloud and data services, thereby ensuring a distributed system where the data is shared across nodes. This digitalization of the shop floor is achieved through the use of integrated platforms that make modern solutions faster, safer, transparent, and more efficient compared to their conventional counterparts [23]. The IIoT devices attached to the machines enable them to trade information on their tasks and progress to the cloud through the blockchain system. The gadgets also enable machine to machine communication in the IIoT network and hence machines can optimize their run time and tasks accordingly.

The IIOT devices used in the network primarily consists of two layers: The interface board and a single-board computer (SBC). The interface board has digital and analog I/O functionalities with which the sensors and actuators interact. The interface board and the single-board computer are connected by serial ports and a series of sensors.

The sensors and application drivers are installed in the SBC and they subsequently enable the use of the sensors and actuators to their maximum potential as the drivers are frequently updated and customized according to the current requirements. The SBC can be edited and designed according to the requirements of the user using gadget supervisor present in the SBC. This is possible using a web interface that can also be used to monitor the status of the devices. Moreover, the I/O unit present on the SBC can act as an interface to connect the blockchain-IIoT platform to external networks.

Figure 7.1 depicts the architecture of the proposed blockchain-IIoT system [23] that incorporates an interface board and a single-board PC. Sensors and actuators interact with the interface board that has a sequential interface to the SBC and with the machine. The sensors help establish a connection between the interface board and the SBC and they enable the SBC to receive sensor information from the interface board and send control signs to the actuators.

The blockchain administration on the SBC communicates with the blockchain network by issuing and receiving exchanges to and from the system. Each IIoT gadget has its own record on the blockchain network and maintains a blockchain wallet on the SBC. These records can be easily accessed and their identity can be verified to ensure integrity of the network. The controller administration is used to monitor machine status, working condition, and transmit exchanges to the smart contracts on the blockchain [24].

Figure 7.2 illustrates how users interact with modern industrial systems using the blockchain-IIoT interface [23]. The industrial systems consist of machines and

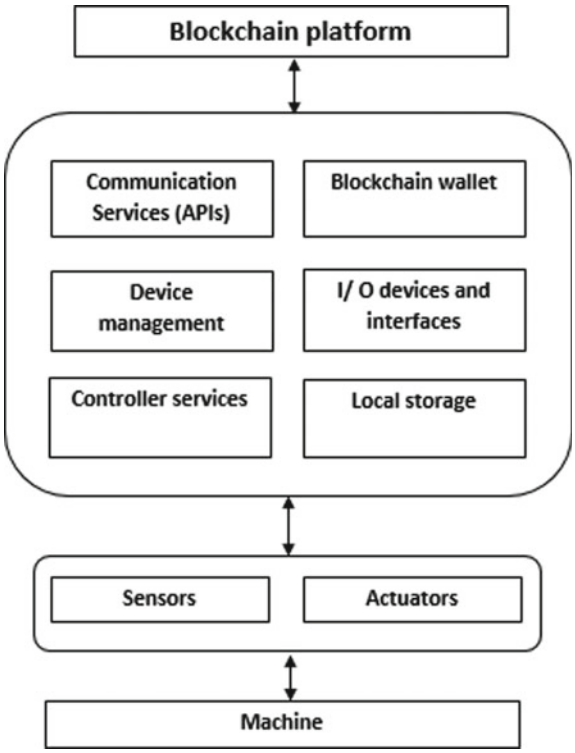

Fig. 7.1 Proposed blockchain-IIoT platform

devices that are connected and grouped together to form ensemble applications. The proposed platform is connected to the cloud to store the data and perform analytics. However, the transactions between the user, cloud and the system are processed through the distributed blockchain network which essentially acts as an interconnecting entity. This blockchain offers excellent scalability as more blocks can be added as the network size and number of transactions increase. Furthermore, since blockchains are essentially peer to peer networks, the chain scales with the increase in the number of users.

7.4.1 Summary of Other Blockchain-IIoT Platforms

Although blockchain technology is relatively new, its benefits and applications have been widely realized by organizations and they have developed blockchain platforms in IIoT. These platforms are created by either integrating the technology with an existing IIoT system or developing a new ensemble system altogether from scratch.

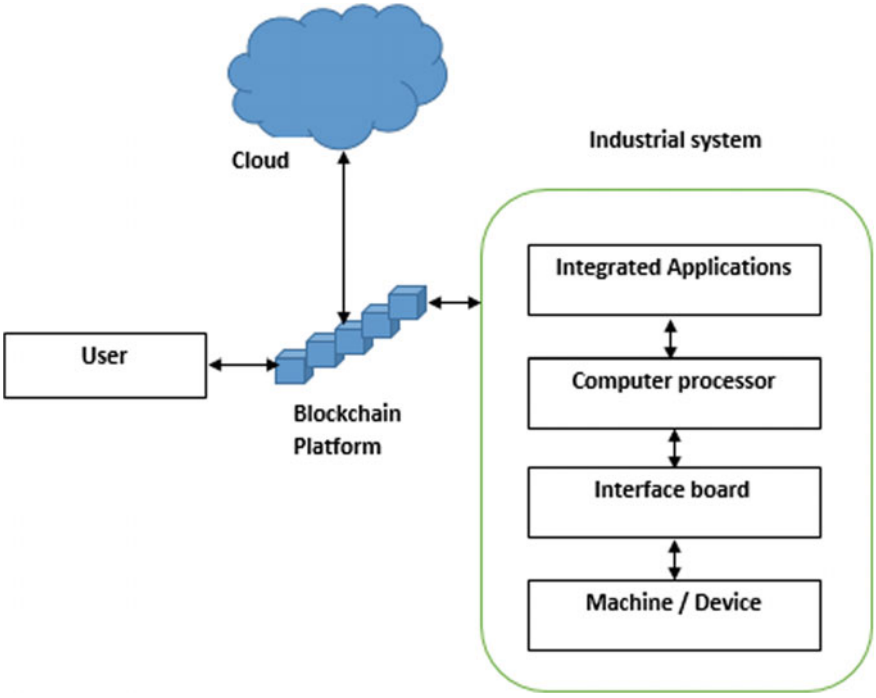

Fig. 7.2 User interaction with blockchain platform

Some of these platforms implemented in the industrial sector are well established, proven, and stable.

The hyundai digital asset company (HDAC) [25] applies blockchain technology to rapidly and securely transmit data, perform verification and information stockpiling between IoT gadgets. The innovation is connected to industrial facilities and devices to facilitate machine-to-machine exchanges and activity between IoT gadgets. The system consolidates a twofold chain framework (open and private) to build exchange rate and volume, which makes it suitable for IIoT ecosystems. HDAC provides users with the option to select their own transaction fees and allows them to create smart contracts themselves. Moreover, this flexibility is further enhanced by the decentralized approach used by the company in offering IoT data control systems. It also offers transactions through other blockchain systems such as Bitcoin and Ethereum.

VeChain [26] is a global blockchain project that provides IoT-based solutions by ensuring secure collection, management, and exchange of data. The blockchain is utilized in an assortment of routes, with one spotlight being on IoT-based solution in cold chain logistics by utilizing IoT devices to monitor key parameters. Among other applications, the platform can hold car visas by making computerized records of vehicles including fix history, protection, enlistment, and driver conduct all through its lifecycle. Social insurance applications are additionally conceivable by utilizing start to finish following of generation procedures of restorative gadgets; and enable

patients to safely share their biometric information with their specialists to empower constant checking. VeChain [26] utilizes IoT innovation for extravagance merchandize by implanting smart chips in luxury goods for real-time tracking of sales.

Waltonchain [26] is a blockchain platform that is made through a mix of RFID and blockchain advances for successful IoT integration. It is focused on tracing procedures and items in the inventory network. The system involves the concept of merging production line garments, applications, equipment, and managing asset by embedding RFID labels and chips into items. Data with respect to the status of items is then downloaded for examinations onto a protected blockchain.

Ethereum [27] is an open-source blockchain platform that allows user to deploy decentralized and distributed solutions. It uses Ethereum as its crypto currency that is used by miners to pay for transaction fees and services. Ethereum offers excellent support for smart contracts and allows users to create their own applications to perform customized operations. It uses innovative computer software called Ethereum Virtual Machine (EVM) that enables any user to run applications and programs in the blockchain network regardless of the programming language. Ethereum can be used to build decentralized autonomous organizations (DAOs) that are organizations run by software on a system of smart contracts in the blockchain network. DAOs do not have a single leader and are owned by everyone who contributes to it and interact with it by buying tokens. Ethereum is also being used as a secure and reliable platform to launch cryptocurrencies. This is possible, primarily due to the fact that the transactions and digital assets are governed and tracked by special standards such as ERC20 and ERC721. Ethereum is rapidly accelerating the decentralization of the world's economy with its user-friendly, reliable, and secure platform.

7.5 Use Cases of Blockchain in IIoT

Blockchain-IIoT integrated systems have already seen a variety of use cases in the industrial world. Organizations have designed, tested, and implemented blockchain and IIoT-based solutions in areas such as transportation, logistics, pharmaceutical industries, and manufacturing factories. This level of acceptance and widespread implementation of blockchain in IIoT systems are primarily due to its unmatched security, transparency, and privacy. This is an especially important factor, provided the volume of sensitive and critical data that modern systems tend to handle.

However, the lack of strong cybersecurity remains one of the major hurdles in the full adoption of IIoT systems. Moreover, industries need auditability and transparency to track and monitor their transactions and this is provided by blockchain. With the integration of blockchain with IIoT systems, organizations are more confident and keener on shifting to such modern systems.

7.5.1 Security and Privacy in Supply Chain Management

IIoT and blockchain can push the boundaries of supply chain management (SCM) systems and enhance their operational efficiencies. In modern SCM systems, numerous sensors track key parameters such as temperature, location, vibrations, humidity, level, and orientation of the object, etc. Since these devices share information and communicate with each other, they can use smart blockchain contracts to secure the transmitted data, stored information, and record the transactions performed.

Blockchain systems depend on cryptographic calculations intended to avoid information contortion. Since each block in a blockchain contains a hash to the previous block, it is extremely difficult to alter the chain. Any changes made to a single block have to be done on the entire network and hence, it offers excellent security to the IIoT ecosystem [28].

Figure 7.3 shows an exchange between a purchaser and dealer in a store's supply chain network [29]. The interaction is processed through the blockchain network and the transmission occurs in the form of smart contracts. The blockchain network contains system information such as the inventory level, purchase order, shipping manifest and invoices. When an input is received, it is matched with the records stored on the blockchain platform and once verified, the transaction is performed.

The need for a viable data sharing method and trust in supply chains fuels the enthusiasm for inventory blockchain networks. Moreover, blockchain networks have enhanced information sharing and security protocols compared to conventional systems [30].

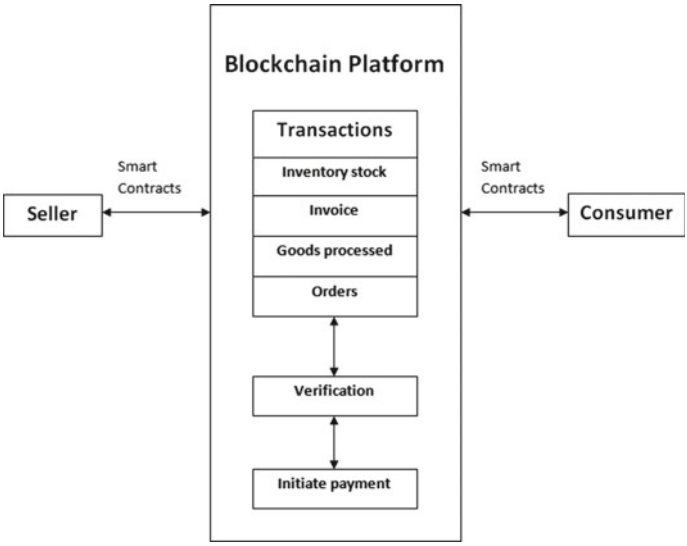

Fig. 7.3 Blockchain in SCM

In blockchain, records are created and stored and they contain information about everything from the stock, source, and destination to the details of the transactions and the entities involved in the transaction.

Stakeholders can view and verify the details of the products at a retailer, such as credibility, quality, quantity, models, reputation of manufacturer, reliability, cost, etc. This also facilitates the continuous monitoring and tracking of shipments throughout their journey. Moreover, due to the distributed nature of blockchains, it is less demanding to access and process data as the data does not have to pass through a central system every time.

The danger of shipment information being adjusted coincidentally or intentionally is a major issue in supply chain systems. Blockchain helps to recognize mistakes or alteration in production network records. Blockchains are extremely resilient to alterations and changes in the network and modifications can be immediately identified. Although blockchain frameworks enable users to view or add information to a record, they cannot alter or erase existing areas in a record. Changes made to records are identified and all the stakeholders are notified with a perpetual log of the changes made.

7.5.2 Pharmaceutical Industry

The issue of counterfeit medicines in the pharmaceutical sector is increasing with every passing day. The pharmaceutical industry is responsible for developing, manufacturing, and distributing drugs. It is essential to monitor the complete journey of the drugs from the manufacturer to the patient. This is to ensure that counterfeit drugs are not mixed with authentic ones and also to monitor the effectiveness of the drug on the general population. However, this is an extremely difficult task that is often rendered impossible using conventional systems. But the transparent and auditable nature of blockchain technology can help in monitoring the shipment of drugs from its origin to the destination in the supply chain.

Blockchain and IIoT-based systems can be designed to track the legal chain of ownership of prescription medicines. Transparency and traceability are essential when it comes to monitoring sensitive healthcare products. The data stored on the distributed ledger is immutable, time stamped, and secure. This data is accessible by manufacturers, wholesalers, dispensers, and end-customers involved in the supply chain. This ensures that individual drugs can be tracked and monitored throughout their journey using blockchain [31].

7.5.3 Autonomous Vehicle Solutions

Autonomous vehicles are fitted with thousands of sensors that collect huge volumes of data on the speed of the vehicle, nearby vehicles, pedestrians, wear and tear in

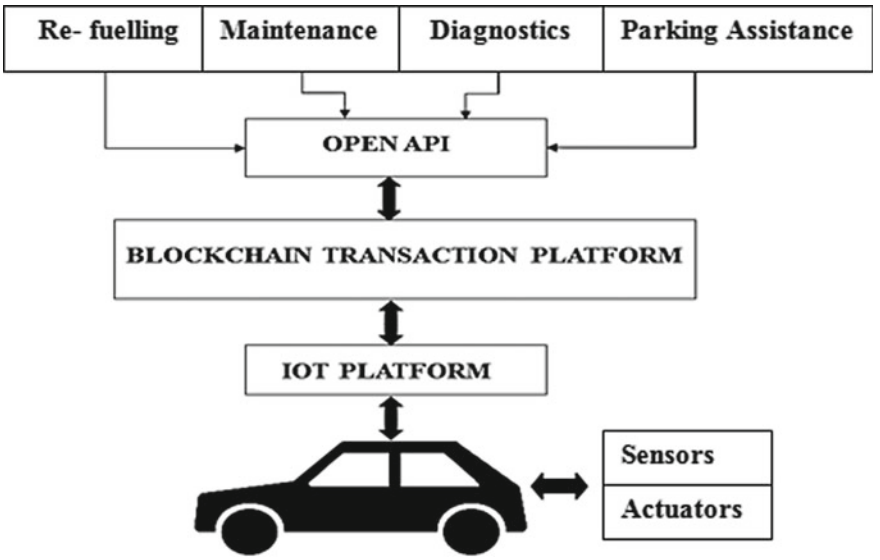

Fig. 7.4 Blockchain-IIoT autonomous vehicle platform

the system, tire grip, proximity to objects, lighting condition, and so on. This data is collected, processed, and analyzed to ensure a smooth driving experience. Figure 7.4 depicts such a system where an autonomous vehicle is embedded with sensors and actuators [32]. The data from the sensors are transmitted to the blockchain network using IoT and is processed to take appropriate decisions.

When the onboard sensors detect anomalies and identify component that could potentially fail, the system can use that information to direct the vehicle to the nearest repair garage. Vehicle manufacturers have plenty of historical data available in the blockchain and this can be utilized for conducting predictive maintenance.

The IIoT layer interacts with the blockchain layer and fetches the appropriate historical data from it, depending on the input from the IoT sensors. Transactions are performed based on this information and are again recorded and stored. This enables data to be stored and accessed in a secure manner and thereby increases the privacy and security protocols in autonomous vehicles.

7.5.4 Manufacturing Process Management

Blockchain and IIoT-based integrated arrangements are used in the production sector to manufacture and assemble mechanical parts and components. Sensors placed in the machinery monitor key metrics such as temperature, pressure, and vibrations and identify deviations from the normal expected behavior. Information received on the blockchain from the sensors is utilized to identify patterns in the anomalous activity

and derive insights from it. This helps in proactively identifying malfunctions and subsequent breakdowns before they actually happen. Such systems are extensively used in the manufacturing of gears where the machine is embedded with multiple sensors that monitor the cut angle, cut depth, temperature, coolant flow, vibrations, and cutting speed.

The information derived from these sensors is transacted through the blockchain system and is subsequently used to monitor the processes. This leads to optimized performance, improved manufacturing quality, and higher reliability throughout the lifetime of the gear. Maintenance workers can monitor the performance of any component in the system by screening the data in the blockchain and can perform preventive maintenance. These observations are also recorded and stored in the blockchain to be used as historical data for further analysis [11].

7.6 Conclusion

IIoT facilitates automated and computerized exchange of data, and this data often has sensitive and proprietary information. IoT devices also tend to have poor processing power, very simple architecture, and minimal storage capacities. This causes available resources to be focused on the core functionalities and thereby overlooking security and privacy vulnerabilities. Attackers tend to utilize these vulnerabilities to compromise the security of the system and gain access to confidential data. Conventional security defense systems tend to have centralized security architectures that are computationally expensive, difficult to audit and vulnerable especially as the number of connected devices increases. These issues can be addressed by blockchain with its secure, distributed, and decentralized approach.

Blockchain with its distributed block system ensures that transactions are swift, secure, and private. It provides excellent resilience to attackers as blockchains cannot be tampered or edited. Its continued integration with the IIoT architecture is already leading to significant transformations across multiple industries, bringing new business models and facilitating reconsideration of how existing systems and processes are implemented.

Moreover, blockchain can also be used to transfer information and allocate resources between devices to efficiently control and manage them. Although there are challenges in introducing blockchain into mainstream industries mainly due to computational costs, transaction verification and issues of integration, its future in the IIoT landscape looks extremely promising.

References

1. Evans PC, Marco A (2016) Industrial Internet: pushing the boundaries of minds and machines. Accessed Jan 2019
2. Zaouini M (2017) Nine challenges of Industry 4.0. https://iiot-world.com/connected-industry/nine-challenges-of-industry-4-0/. Accessed Jan 2019
3. Skarmeta AF, Hernández-Ramos JL, Moreno MV (2014) A decentralized approach for security and privacy challenges in the Internet of Things. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp 67–72
4. Atamli AW, Martin A (2014) Threat-based security analysis for the internet of things. In: International workshop on Secure Internet of Things (SIoT). IEEE, pp 35–43
5. Christidis K, Devetsiokiotis M (2016) Blockchains and smart contracts for the Internet of Things. IEEE Access 4:2292–2303
6. Das ML (2015) Privacy and security challenges in Internet of Things. Distrib Comput Internet Technol 33–48
7. Miraz MH, Ali M (2018) Applications of blockchain technology beyond cryptocurrency. Ann Emerg Technol Comput (AETiC) 2(1):1–6
8. Crosby M, Pattanayak P, Verma S, Kalyanaraman V (2016) Blockchain technology: beyond bitcoin. Appl Innov 2:6–10
9. Conoscenti M, Vetro A, De Martin JC (2016) Blockchain for the Internet of Things: a systematic literature review. In: IEEE International conference on computer system applications, pp 1–6
10. Kshetri N (2017) Can blockchain strengthen the Internet of Things? IT Prof 19(4):68–72 (Article ID 8012302)
11. Wu D, Thames JL, Rosen DW, Schaefer D (2013) Enhancing the product realization process with cloud-based design and manufacturing systems. J Comput Inf Sci Eng 13:1–14
12. Skwarek Volker (2017) Blockchains as security-enabler for industrial IoT-applications. Asia Pac J Innov Entrepreneurship 11(3):301–311
13. Gross H, Holbl M, Slamanig D, Spreitzer R (2015) Privacy-aware authentication in the Internet of Things. Cryptology and network security. Springer International Publishing, pp 32–39
14. Sharma TK (2018) How does blockchain use public key cryptography? https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography, Accessed Feb 2019
15. Huh S, Cho S, Kim S (2017) Managing IoT devices using blockchain platform. In: 19th IEEE international conference on Advanced Communications Technology (ICACT 2017), pp 464–467
16. Colombo A et al (2014) Industrial cloud-based cyber-physical systems. The IMC-AESOP Approach, Springer, Switzerland
17. Banerjee M, Lee J, Choo KKR (2018) A blockchain future to internet of things security: a position paper, Dig Commun Netw 4(3):149–160. Aug 2018
18. Teslya NN, Igor R (2018) Blockchain platforms overview for Industrial IoT purposes. In: FRUCT'22 Proceedings of the 22st conference of open innovations association FRUCT, Article No. 35
19. Luu L, Chu DH, Olickel H, Saxena P, Hobor A (2016) Making smart contracts smarter. In: Computer and communications security, Vienna, Austria, ACM, pp 254–269
20. Brody P, Pureswaran V (2014) Device democracy: saving the future of the Internet of Things. IBM. Accessed Jan 2019
21. Miraz DR (2017) Blockchain: technology fundamentals of the trust machine. https://doi.org/10.13140/rg.2.2.22541.64480/2
22. Jesus EF (2018) A survey of how to use blockchain to secure Internet of Things and the stalker attack. Secur Commun Netw 2018:27, Article ID 9675050
23. Bahga A, Madisetti VK (2016) Blockchain platform for Industrial Internet of Things. J Softw Eng Appl 9:533–546
24. Petracek N (2018) Is blockchain the way to save IoT. Forbes Technology Council. Accessed Jan 2019

25. Buck J (2017) Bringing blockchain to IoT. https://cointelegraph.com/news/bringing-blockchain-to-iot. Accessed Jan 2019
26. Chrisjan P (2018) How significant is blockchain in Internet of Things? https://cointelegraph.com/news/how-significant-is-blockchain-in-internet-of-things/. Accessed Feb 2019
27. Ameer R (2017) What is Ethereum? The most comprehensive guide ever! https://blockgeeks.com/guides/ethereum/. Accessed Feb 2019
28. Dickson B (2016) Blockchain has the potential to revolutionize the supply chain. Aol Tech, Accessed Jan 2019
29. Rooyen JV (2017) Blockchains for supply chain—part 1. https://resolvesp.com/blockchains-supply-chains/. Accessed Jan 2019
30. Kshetri N (2018) Blockchain's roles in meeting key supply chain management objectives. Int J Inf Manag 39:80–89
31. Chaudhuri A, Jochumsen ML (2018) Blockchain's impact on supply chain of a pharmaceutical company. In: EUROMA conference 2018, Hungary
32. Laplante PA (2018) Blockchain and the Internet of Things in the industrial sector. Accessed Jan 2019