Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM

ISSN: 2788-7421

Blockchain-Technology-Based Solutions for IOT Security

Israa Al-Barazanchi[1,2,*], Aparna Murthy[3], Ahmad Abdul Qadir Al Rababah[4], Ghadeer Khader[5], Haider Rasheed Abdulshaheed[1], Hafiz Tayyab Rauf[6], Elika Daghighi[7], Yitong Niu[8]

[1]Baghdad College of Economic Sciences University, Baghdad, Iraq
[2]College of Computer Science & Information Technology, Universiti Tenaga Nasional (UNITEN), Malaysia
[3]Professional Engineers in Ontario, North York, ON M2N 6K9, Canada
[4]Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh 21911, Saudi Arabia
[5]Masters of Applied Sciences in Engineering Physics
[6]Centre for Smart Systems, AI and Cybersecurity, Staffordshire University, Stoke-on-Trent, United Kingdom
[7]Technical and Vocational University, Tehran, Iran
[8]Belarusian-Russian University, Mira Avenue 43, Mogilev, 212000, Republic of Belarus

*Corresponding Author: Israa Al-Barazanchi

DOI: https://doi.org/10.52866/ijcsm.2022.01.01.006
Received October 2021; Accepted November 2021; Available online January 2022

ABSTRACT: After a long period of development, blockchain innovation has received much attention from scholars and industry practitioners alike. This innovation allows the issuance of smart contracts, which are utilised to automate and execute deals amongst clients. Blockchain is also being used nowadays by a few IT applications as a specialised foundation. This technology also prevents the duplication of information similar to what is being done with Bitcoin and other cryptocurrencies. Specifically, Bitcoin records are virtually impossible to alter as this cryptocurrency is being traded amongst hundreds of thousands of servers. Therefore, to launch a successful attack, the aggressor should change the Bitcoin records of 51% of these servers simultaneously. The cost of such effort significantly exceeds the potential payoff. Meanwhile, private data that are stored on single servers, such as Amazon and Google, are prone to malicious attacks. Therefore, in this paper, we propose the use of blockchain to solve the security issues in the Internet of Things (IOT). We initially identify and categorise the prevalent security issues, particularly data privacy, being faced in IoT in expansion to conventions utilized for organizing, communication, and administration. Afterwards, we formulate some security measures for IoT and illustrate scenarios where blockchain is being used in IoT applications.

Keywords: Blockchain; IoT security; Blockchain technology; Network security; Data security

1. INTRODUCTION

Blockchains use cryptography to connect records or ‘pieces’, with every piece containing a timestamp, the cryptographic hash of the previous block and the information or ‘Merkle tree’ to be exchanged. The information contained in a blockchain cannot be adjusted, can only be recorded once and cannot be changed retrospectively [1]. A blockchain facilitates a rapid development of applications without the need to build trust amongst peers. This type of innovation has gained worldwide popularity given its unchanging nature and its ability to ensure the non-denial and responsibility of putting away data. The wide accessibility of information on computer networks also introduces challenges related to managing and handling large amounts of information with low latencies. Along with the advancement of blockchains, artificial intelligence and machine learning techniques have witnessed noteworthy enhancements, thereby facilitating

*Corresponding author: israa44444@gmail.com, israa.albarazanchi@baghdadcollege.edu.iq their use in subsequent generation systems. Accordingly, this article examines these innovations that contribute to the development of highly dependable computer systems and knowledge-powered defence applications. Web giants, such as Amazon, Facebook, Google, Microsoft and Apple, store most of their critical information in centralised servers. Therefore, attackers aiming to steal or manipulate such data know exactly where to launch their attacks. To this end, blockchains have been used to build security within the Internet of Things (IoT) [2]. Apart from blocking attacks, blockchains also prevent the unauthorised duplication of information similar to what is being done for Bitcoin and other cryptocurrencies. Given that Bitcoin records are put away by hundreds of thousands of servers, they are unable to be manipulated. To launch a successful attack, the aggressor needs to manipulate the records stored in 51% of these servers simultaneously, and the cost of such attack greatly outweighs the payoff. However, the same cannot be said about the private data of individuals, which are typically stored in single servers that are hosted by Google and Amazon. Security is a persistent problem in IoT given its largely loose IoT market. Accordingly, security has also become a concern for smart devices, such as smart homes and smart cars. For instance, a hacker may make unauthorised purchases or operate a self-driving car with other passengers onboard by using the entry levels given to an IoT system. Therefore, the data being traded across IoT devices require strong security [3]. Apart from the currently available security measures used in IoT devices, such as two-factor authorisation and biometrics, blockchain IoT security has been identified as an interesting solution to IoT security problems given its proven performance in guarding cryptocurrencies from being manipulated, blocking authorised users from accessing the IoT and shutting down compromised devices in an IoT network. Hyundai recently launched its blockchain start-up, the Hyundai Digital Currency (HDAC), which is specifically designed for guaranteeing security in IoT and private networks [4, 5].

2. BLOCKCHAIN TECHNOLOGY

2.1 BLOCK BODY

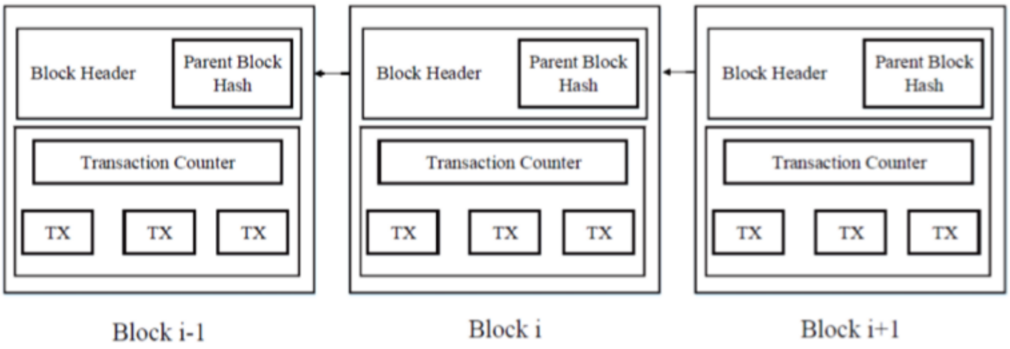


FIGURE 1. **A blockchain comprising an uninterrupted sequence of blocks.**

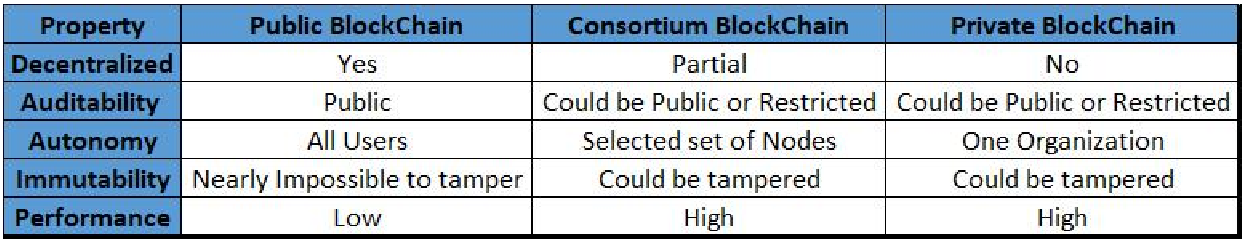
Blockchain shows high potential to be implemented by companiesto achieve a secure exchange of informationin 2009, for Bitcoin benefitting blockchain technicality, thither have it been expanding numeral of blockchain technically based Processors.A ban arrangement of piecesdaeach other in a work topologya persistent grouping of squares [6].

Blockchains are primarily implemented using electronic frameworks that allow a global exchange and conveyance of information or records via cryptography. Each exchange is denoted by an asymmetrical key set. The exchange date effectively and safely archives a group of occasions at a road to each endeavor to alter or alter a past exchange will moreover demand a recalculation from all consequent squares of exchanges [7]. Instead of building trust amongst peers, blockchains rely on four key features, which are described as follows [8]:

- Ledger: a technicality employment an add as it were recorded to equipping full value-based history. Not at all like traditional databases, are exchanges while values at a blockchain not been overruns.
- Secure: Blockchains are encrypted, thereby ensuring that the information stored therein cannot be manipulated without authorisation.
- Shared: Each record involves numerous members. This is gives straightforwardness over a hub member within a blockchain web.
- Distributed: A blockchain may be disseminated, and the number of nodes in a blockchain can be calibrated to increase its flexibility and to reduce the possibility of a successful attack.

The identities of blockchain users are also kept anonymous and are associated with various identifiers. All exchanges taking place in a blockchain are visual. This has viably empowered Bitcoin to display bogus-anonymity since computation

Table 1. **Comparison amongst public, consortium and private blockchains.**



Property	Public BlockChain	Consortium BlockChain	Private BlockChain
Decentralized	Yes	Partial	No
Auditability	Public	Could be Public or Restricted	Could be Public or Restricted
Autonomy	All Users	Selected set of Nodes	One Organization
Immutability	Nearly Impossible to tamper	Could be tampered	Could be tampered
Performance	Low	High	High

ability be made wanting each distinguishing proof or license handle (these forms are ordinarily wanted via "Know-Your-Customer (KYC)"). Ago Bitcoin as if anonymity, he was basic into having instruments into form believe at an climate wherever clients may not exist effortlessly distinguished. Earlier at the utilize of blockchain technology, such believe was regularly conveyed meantime mediators confidence through both parties.

2.2 CHARACTERISTICS OF BLOCKCHAIN TECHNOLOGY

Blockchains serve numerous purposes depending on several properties as summarised in Table-1, which presents a comparison amongst public, consortium and private blockchains [9].

Whilst built on sound and largely understood cryptographic standards, the use of blockchain remains at its infancy. This technology is partly surrounded by build-up, to which several solutions have been proposed. Moving fore, it is probable while the buildup shall pass on down, and blockchain technology shall ended up adjuster another tool that can be used.

2.3 APPLICATIONS OF BLOCKCHAIN

Blockchains have several applications, the most common of which are illustrated in Figure 2. These applications are generally categorised into finance, IoT, public service, reputation system and security [10].

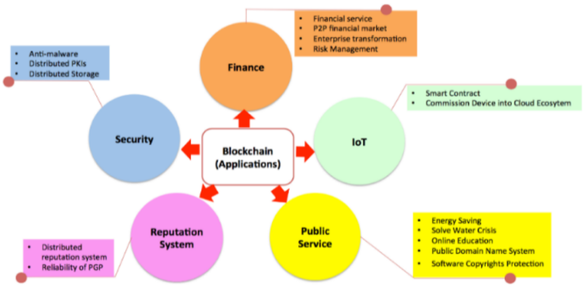


FIGURE 2. **Representative blockchainapplication domains.**

2.4 SAFETY ISSUES IN BLOCKCHAINS

Amongst its several aspects, the safety of blockchains, which is largely based on ‘public ledgers’ and ‘distributed unanimity’, has received the most attention from researchers and practitioners. Blockchains are not immune to all types of extortion and hacking attacks. This technology comprises decentralised and conveyed records that can be exchanged over several hubs. Blockchains may be implemented peer-to-peer in the presence of a trusted third party. The information stored in a blockchain are protected from attacks via cryptography. Due to their nature, blockchains are expected to be used to solve network attacks in the future. The foremost imperative protection the case of the blockchain Support framework is also known as 51% attack. Bitcoin procedures and the level of computing action, organize in Fixes of the retail rate. When more than 51% of the retail rate is regulated by a single hub, the information contained in blockchains may be malevolently manipulated. In this 51% assault, 2 clashing squares compete for space in the same blockchain [11]. Through their frameworks, blockchains have demonstrated an exceptional performance in predicting objective data extortion attacks. whitening assaults, ballot stuffing beneath sybil assaults, consistent assaults and disguised assaults [12]. Whilst central information stock and administration frameworks are vulnerable to piracy, interruption and breakthroughs problems, blockchains anticipate the future occurrence of piracy attacks. Therefore, all transactions in a blockchain should be confirmed by servers, and false exchanges should be identified and terminated. Given that blockchains always monitor an entire arrangement of hubs, assaulters are given no chance to embed false squares in blockchain records and launch a successful attack [13].

2.5 REQUIREMENTS AND ADVANTAGES OF BLOCKCHAINS

Requirements engineering (RE) plays a key role in software development. However, requirements engineers are unable to effectively contribute to software development when stakeholders are generally unknowledgeable about RE techniques.

As a major activity in RE, requirements traceability (RT) involves engineers attempting to verify if the software requirements have been properly determined throughout its development life cycle. Despite its introduction in 1994, RT still lacks mature processes and has still not received wide adoption in software development.

RT automation utilises a wide range of technologies, most of which are developed based on information retrieval (IR) techniques, such as the vector space model. However, IR-based models have limited precision. To improve the precision of these models, other tools have been developed, including the feature-oriented tool that accurately traces the requirements automatically [14]. Blockchains have also been used to address challenges in software engineering, hence leading to the introduction of blockchain-oriented software engineering. However, blockchain-oriented software engineering requires the adoption of standard techniques being used in software engineering and has received limited research attention thus far. Nevertheless, blockchain-oriented software engineering is widely believed to simplify the communication amongst stakeholders, help organisations manage software development requirements and improve the accuracy of the RT process by creating a distributed environment wherein stakeholders can reach a consensus on RT strategies without using tracing tools or requiring third parties who can control the entire RT process [15]. Blockchains have also been used in other industries to solve various problems, such as in data processing, data security, data transparency and data reliability. Given its decentralised characteristics, a blockchain effectively avoids the monetary and time costs that are usually involved in database security maintenance because the transactions taking place in a blockchain can be independently processed and verified without third parties, hence limiting the risks of malevolent attacks [16]. The participants in a blockchain may also involve themselves in decision-making processes and are given the power to control the transactions and all other information available on the blockchain. These participants can also access all the actions and data stored in a blockchain, which are sent to all computers connected to the network and are unable to be modified or deleted. Given these advantages, a blockchain has been described as a trustworthy, immutable and transparent technology [17].

To further enhance security, all participants in a blockchain are assigned a unique identity. The cryptographic hash being used in a blockchain demonstrates exceptional reliability and security because each time a new block is created, a new hash that includes the unchangeable value of the previous hash is automatically generated. Blockchains are also known for their faster processing speed compared with existing technologies. Specifically, previous technologies require approximately three days to process a transaction, whereas blockchains complete each transaction within seconds or minutes. However, blockchains also have their own challenges, one of the most common is their high energy consumption for keeping real-time records and for verifying transactions. Such high energy consumption corresponds to high transaction costs. Nevertheless, the benefits of blockchains greatly outweigh their disadvantages [18, 19].

3. IOT

IoT collectively refers to seamlessly connected devices that communicate with one another via the Internet. The increasing number of modern-day devices that are connected to the Internet, including digital assistants (e.g. Alexa and Siri), refrigerators, measurement sensors and lighting equipment, continuously blurs the boundary between Wi-Fi-enabled devices and other devices [20]. Massive amounts of data are being generated by billions of embedded Internet-enabled sensors from various domains worldwide. These data are being used for analytics, for monitoring operations and for reducing the number of manual processes. In this case, IoT aims to achieve a seamless connection amongst devices and to generate data that can help businesses overcome hurdles in their processes and understand the preferences of their consumers. IoT is most commonly used in mobile clouds that interact with one or more mobile devices [21].

Consumer IoT includes smart home and wearable devices that are specifically marketed to consumers. These devices not only provide consumers with improved experience and efficiency but also create health and safety benefits [22]. For instance, using IoT devices can help consumers efficiently conserve energy, control the climatic conditions in their homes, increase their agricultural produce and manage their inventories. Some health and safety benefits of IoT include early disaster warnings, environmental excellence and caregiving. Both IoT and cloud computing serve many traditional applications and have paved the way for the construction of smarter homes and cities. IoT and cloud-based management systems aim to providing realistic solutions to problems through the deployment of sensors to capture data that will are transmitted to a cloud sever in real time for storage and secondary analysis. These sensors can be remotely controlled by administrators of Internet-based human–machine interface to serve a variety of applications. Meanwhile, machine learning techniques facilitate the analysis of sensory data based on feature extraction. Powerful computing resources, such as GPU, are evolving in neural networks and the cloud environment. The advantages of IoT in data collection have also been leveraged in anomaly detection tasks [23, 24].

3.1 COMPONENTS OF IOT

An IoT system has four major components, namely, sensors or devices, connectivity, data processing and user interface (UI), as described below:

Sensor/devices: Sensors or devices are basic elements of an IoT that collect data from devices with an Internet protocol (IP) address. These devices may be as simple as temperature/humidity sensors installed in buildings or as complex as intelligent vehicles. These components mainly serve the purpose of collecting data, such as temperature or video, in their respective environments. Instead of operating independently, these sensors/devices are bundled together. An IoT structure comprises devices that can collect information from physical environments and transmit such information to the IoT ecosystem. Sensors may be deployed in various environments, such as healthcare (e.g. to monitor the vital signs of patients) or industry (e.g. to monitor temperature or pressure). Generic devices, including Raspberry Pi and Arduino-embedded systems, enable the customisation of IoT end points [25].

Connectivity: Sensor and other devices are connected to a cloud by using various types of networks, including LAN, Wi-Fi, satellite, Bluetooth and cellular infrastructure. Therefore, IoT devices utilise standard communication protocols to communicate with one another. For example, Bluetooth low energy (BLE) or Wi-Fi are especially designed for IoT stream. Increasing the bandwidth and speed of the 5G cellular network is expected to benefit IoT [26].

Collecting massive amounts of data has necessitated the introduction of new technologies, such as edge computing, which is a new model for distributed devices. In edge computing, both the data and the power of computation are allocated to where they are needed the most. Any information that the filtered cloud does not process is moved closer to the consumer, thereby increasing bandwidth and reducing lag time. The data are processed by these machines or systems, and only the most relevant pieces of information are transmitted back to the central base for analysis. For example, each camera in a surveillance camera system outputs 3 Mbps at 30 fps. Each frame with a size of 100 kb bombards the security operations centre, which in turn uses these frames for video streaming. Edge computing helps the security operations centre in this example by analysing the incoming video and sending alerts each time movement is detected [27].

Data processing: After being stored in the cloud, the data are processed with the help of software. Before they can be of any use, these collected data should be processed, filtered and analysed in a specialised manner. To prevent the system from being overwhelmed, zettabytes (10^{21}) of data are guided thru each edge gateway before they can be processed. In this example, IoT is used to collect information from real-world environments through sensors in order to formulate real-time agile decisions. Big data analytics is applied to analyse production data at the highest level by connecting the enterprise software to the cloud data. The data generated by IoT have varying structure and are real time in nature. Before they can be utilised in decision making, large amounts of IoT-generated data need to be processed, analysed and classified. Therefore, several techniques for identifying and converting raw data into usable forms need to be devised. Some of these techniques include machine learning and artificial intelligence, both of which have been used in [28].

User interface (UI): After being cleaned and formatted, the collected data should also be used to alert end users. For example, users need to be alerted about the temperature in cold storage. A UI serves this purpose by allowing end users to proactively check the collected data. Therefore, these end users may also react to the system inputs depending on the IoT applications. For example, after receiving an alert on his/her phone, an end user sends back an input, such as by adjusting certain parameters (e.g. ‘control’ or ‘regulate’ the temperature in cold storage). In some cases, instead of waiting for input from the user, some actions can be automated. For instance, instead of waiting for input from the user, the temperature in cold storage can be regulated based on a set of predefined rules. Moreover, in home automation systems, an IoT system automatically sends a notification to the authorities instead of sending an alert to homeowners [29].

3.2 DATA PRIVACY AND SELF-SOVEREIGN IDENTITY

The birth of IoT can be ascribed to the rapid evolution of information technology for measuring and processing data [30]. IoT comprises interconnected physical objects that exchange their data with one another through electronic sensors. The components of an IoT can also send their data to centralised systems of servers or other devices following the extant principles of the data exchange infrastructure. By controlling its own structure and the users presently in the network, IoT facilitates the communication between computer-based systems and the physical world. This technology is specifically designed to facilitate the movement of objects in their physical environments, which can only be realised in the presence of actuators or sensors that allow IoT to support physical cyber applications. Given its dynamism and high mobility, IoT is constantly changing, which entails high risk [30]. Whilst IoT both defines and manages the data for its devices (e.g. user information), the way these data are shared remains unclear [31]. For instance, some IoT data are not easily manipulable and are highly time sensitive, thereby necessitating a more careful treatment. Some data generated by IoT are quite sensitive and are therefore potential targets for aggressors given that such data exposes the entire network to security risks [32]. Along with the continuous, significant development of science and technology, more network data are being accumulated. The main problem of IoT lies not on its security but on the high network traffic or the massive volumes of data being exchanged [33]. Whilst IoT can provide advanced services, this network must also ensure that the information or privacy of its users will not be compromised. For this reason, IoT should guard itself from various types of attacks, such as client denial, eavesdropping and fraud. In addition to the aforementioned capabilities, IoT also has light security features, which generate heavy computational burden in data exchange processes, especially for networked computers [34]. Certain security methods may be inapplicable to IoT given the heterogeneity of dynamic devices and the presence of large-scale, unprotected environments [30]. Privacy remains a challenge in IoT because some objects that are connected to this network may have incompatible structures or may not be designed for such connection. Therefore, the amount of risks in the network increases, which would necessitate the deployment of additional defence techniques. Protecting the privacy of some information systems may also be a challenge. The high security principles observed in IoT include authentication, access control, encryption and role-based access control as will be discussed below [30] [34]:

1. Authentication: By identifying the core of the work, authentication greatly reduces the risk of attacks, such as sibling attacks, scams and compromised privacy.
2. Access control: Through access control, only authorised users are given the right to use IoT.
3. Safe loading technique: IoT adopts the secure download technique to reduce its consumption of computing and storage resources.
4. Malware detection: IoT protects itself from privacy attacks, network disruptions, power outages, viruses, worms and trojans through malware detection.

The following characteristics of IoT also expose the network to additional risks [30]:

1. Dynamic
2. Extremely high mobility
3. No fixed location
4. High heterogeneity
5. High traffic and large volumes of data being exchanged

Despite catching up with the development of any technology, the security features of IoT require further improvement. For example, the introduction of machine learning in IoT was followed by the creation of a defence site that enabled secure, heterogeneous and dynamic data exchanges in line with security protocols. The presence of attacks hampers the detection of IoT given the limited availability of resources [34].

Machine learning

When faced with a problem, IoT responds by selecting the relevant key parameters and security protocols. Machine learning helps IoT establish low volume contact and control protocols that not only extend its life but also conserve its energy. For example, the reinforcement learning (RL) model improves the performance of the system by using authentication and malware detection [34]. As decentralised technologies, blockchains can be used in IoT to improve the transparency of data sharing and auditing the data stored in memory. Given their ability to control smart contracts, blockchains also prevent the privacy of individuals from being compromised by controlling uninterrupted operations independently, thereby reducing network traffic and ensuring continuous operations. Deploying such technology in IoT can also prevent the loss of private information and allow users to send their data directly to the network [31]. Privacy is an unignorable principle in IoT. The identities of users in IoT cannot be disclosed; any act of disclosing such identities can be viewed as forgery. Apart from addressing the problems mentioned above, using strong security techniques in IoT also serves the following purposes [30]:

1. Some companies who use IoT also fail to comply with the security protocols prescribed in the network, which would entail high security costs in terms of financial or compliance with these points, which is due to the existence of bringing the Sank in load into the network.
2. The existing tools and products being deployed in IoT to address security disruption issues are not well established. Specifically, IoT has an imperfect hardware operating system, operates on a limited amount of computing resources and requires high operating costs especially when performing several encryption operations simultaneously to ensure the privacy of information. Given its frequent interactions with many users, another task of IoT is to protect

the privacy of these individuals. Take for example a doctor's office that serves 20 to 30 patients each day. The office inputs the information of each patient into the network, and such information is exclusively for the use of the doctor and his/her patients. However, ensuring the privacy of such information is difficult, hence resembling the situation of IoT users. Such problem can be efficiently solved in IoT depending on the sensitivity of data [30]. Accordingly, protecting the privacy of network users has become a particularly important issue that directly affects the data and the network policy for such data. The following solutions for such problems have been recommended:

PEFM: PEFM is an indirect policy mechanism applied in IoT to ensure the data privacy of users regardless of the sensitivity of such data. This policy essentially seals the network, hence effectively blocking the unauthorised entry of data and preventing the data of users from falling into the wrong hands. PEFM is a policy technology that utilises security mechanisms to ensure that none of the information stored by legal users in the network will be leaked. This mechanism depends on the creation and activation of data and utilises a virtual machine. PEFM is not an executable machine; rather, this operating mechanism is embedded into IoT to avoid the risk of privacy attacks. PEFM employs two methods, namely, apoptosis and evaporation.

On the one hand, upon detecting a fault in the system, PEFM utilises apoptosis to identify the fault by examining the sensitive data. On the other hand, PEFM utilises evaporation when an unauthorised person is detected in the system. Specifically, evaporation implements a specific privacy policy to remove such unauthorised person from the network [32].

Meanwhile, to address the network traffic in IoT, the following solutions have been proposed [33]:

1. Store data in the traditional way
2. Keeping a distributed file and database
3. Cloud computing

Cloud computing is considered a superpower solution that helps users detect the presence of security issues in the network. The failure to protect people's privacy and the sensitivity of data introduce other problems, hence requiring urgent attention. Cloud computing can only be implemented in networks whose security issues are clearly known to users. Consequently, because the method applies to high data volume networks, it should know where to show which reaction [33].

4. BLOCKCHAIN-TECHNOLOGY-BASED IOT

Blockchain has the potential to change how users view security issues in IoT, hence introducing opportunities for users to reconsider issues related to their online personalities. The Internet was not outlined for current exchanges nowadays, and our communication conventions do not have sufficient data around the character of the people or gadgets included in them. The stakes are more prominent than fair keeping mechanical sensors online [35]. Addressing these challenges lead to the introduction of new approaches for creating online personalities, ensuring reliable exchanges and building flexible systems. Blockchains offer many benefits in various areas, such as in production and supply chains. Start-ups use blockchains to monitor the movement of products from their producers to their end users. New commerce models for centralised cloud servers are also being developed. For example, Fiber, as a supplier of blockchain-based IoT arrangements, develops remote sensors that improve the communication of the network with PCs, tablets and smartphones operating within a 16 km distance. Many of these sensors shape low-power autonomous cellular systems that help companies manage their tasks. However, these systems do not employ cloud administration. A secure trading of information amongst gadgets is ensured by using blockchains that store unique identifiers for each hub. Amongst the potential beneficiaries of such development are next-generation mechanical systems. Meanwhile, the blockchain-based apps introduced by Filament utilise independent shrewd contracts and sensors in a decentralized framework [36]. Along with the rise of industrial activities, some financial companies, including the Bank of New York Mellon, Gemalto, Cisco and Foxconn Innovation, have announced their plants to utilise blockchains to ensure security in their IoT. These companies are also planning to develop a blockchain-based convention that contribute to the development of IoT systems, appliances and gadgets. The benefits of combining IoT with blockchains outside of cryptocurrencies have also been proposed. In IoT, the blockchain is considered a missing link that can help solve issues associated with security, scaling and privacy in the network. In 2011, Cisco predicted that approximately 50 billion devices will be connected to and operate on a global Internet network through blockchains by 2020. In their latest forecast released in 2016, Cisco predicted that the number of these devices will increase to 500 billion by 2030. To realise such prediction, companies must spend extravagant amounts on data transmission alone. Moreover, the devices connected to the IoT need to be managed, and their security must be ensured. These efforts introduce problems that hinder the mass adoption of IoT. Figure 3 shows the growth in the number of devices linked to the IoT. In 2008, the number of these devices already exceeded the entire global population, and this number is expected to reach around 50 billion by 2020 [37].

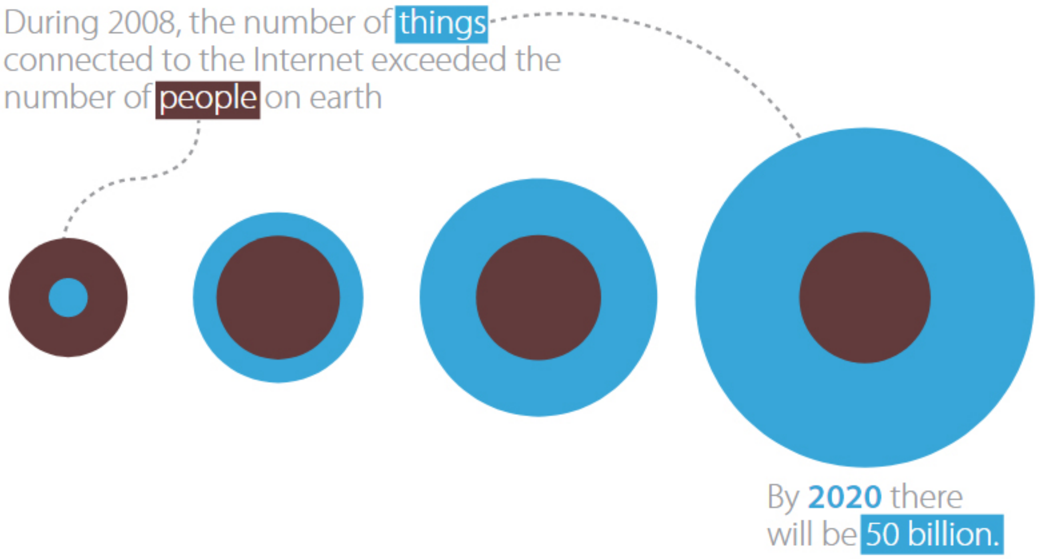


FIGURE 3. **Growth of IoT devices.**

Similar to IoT, blockchain is a relatively new technology, hence explaining why blockchain-based applications have their own limitations. Nevertheless, given their decentralised nature, blockchains offer several advantages that have already been implemented in IoT devices. Moreover, the negative effects of blockchains on the speed of IoT devices have not been supported by any evidence.

5. SCENARIOS OF BLOCKCHAIN USE IN IOT

With their continuous growth, enterprises need to deploy IoT to store their information. IoT based on blockchains has penetrated virtually all aspects of our daily lives, and some consumers are not even aware that they are actively using such technology. One crucial aspect of using blockchains in IoT is the use of cryptographically impervious databases as connection hubs [38, 39].

- **Supply chains**

A supply chain usually involves multiple users operating in different time zones, hence contributing to its complexity. The importance of using blockchains in these supply chains has been recognised in recent years by food distributors, pharmaceutical companies, seaport operators and electronics manufacturers amongst others. Several sectors are also experimenting with revolutionary solutions to their supply chain problems. One of these companies is Samsung Electronics, which is currently the largest producer of smartphones and semiconductors worldwide.

- **Smart appliances**

Smart home equipment is predicted to be a staple in every home in the future. Specifically, new houses and structures are predicted to have several features that can be triggered using smart devices or the Internet. By warding off statistics storage on the predominant server or in cloud storage in choose of blockchain, private statistics can be blanketed and the domestic IoT community might also be secured.

- **Electricity m arkets**

Additionally, statistics from clever units can be used to improve power consumption in the community than at the household or individual level. This option has already received the attention of governments and enterprises. For instance, Siemens partnered with Energy a few years ago to establish a smart grid that utilises blockchain in buying and selling electricity. The Russian authorities have described many degrees towards imposing clever energy. Using blockchain is also expected to ensure the continuous operation of electricity storage structures.

- **Transport**

The transportation industry is currently experimenting with the use of blockchains in IoT, such as in tracing the origins of automobiles and their spare parts. For instance, two of the greatest automobile manufactures in the world, Jaguar Land Rover and Volkswagen, started exploring smart contracts with the aid of IOTA. Specifically, a smart pocket is installed in vehicles, which would allow vehicle operators to earn IOTA tokens in exchange for data on road conditions and congestion and even join carpooling programmes. They may also utilise such tokens to pay for their parking or to charge their electric vehicles. These German automobile producers intend to create a blockchain-based community where automobiles can communicate with one another regarding potential accidents.

- **Smart locks**

Slock, a German company, introduced the Smart Lock technology that uses self-reliant keys in order for to rent, share or sell a wide range of commodities, including homes or flats, bicycles and automobiles. Figure 4 illustrates the framework of this technology.

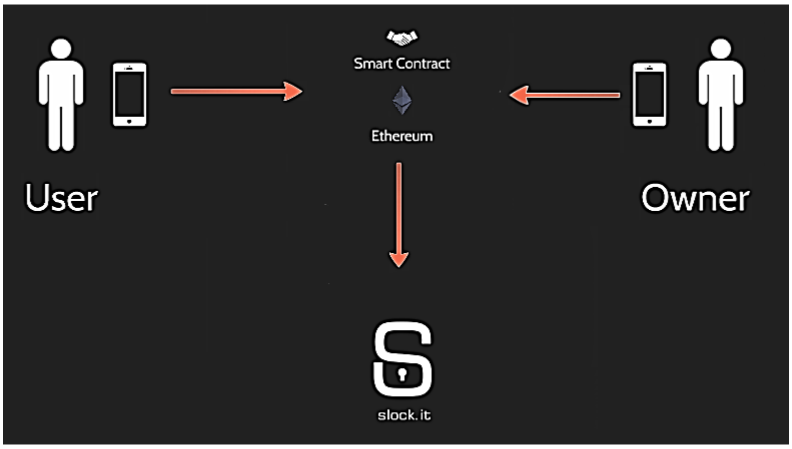


FIGURE 4. **Smart Lock system.**

Take for example a manageable purchaser who needs to pay a deposit, lease and use an item and then return this item to its proprietor to receive earnings that are much less that the associated fees. The entire process is computerised and guided by smart contracts. Each transaction taking place in Smart Lock happens in real time on the EtherChannel blockchain without any interference from a third party and is executed as soon as the lease is approved by using a smartphone [40].

6. CONCLUSION

Blockchains have high potential to be implemented by enterprises to ensure a private exchange of information with a centric specialist. This technology effectively prevents the duplication of information similar to what is currently being done with Bitcoin and other cryptocurrencies. Blockchains also change the way we perceive the security issues in IoT and introduce opportunities for reconsidering those decades-old issues associated with the formation of online personalities. The Internet was not originally designed to serve the current exchanges taking place nowadays. Moreover, recent communication innovations lack sufficient data regarding the characteristics of people or gadgets involved in these exchanges. The stakes are more prominent than fair keeping mechanical sensors online. Addressing such challenges can contribute to the development of new approaches for building online characters, ensuring reliable exchanges and building flexible systems. This paper presents an overview of blockchain as a solution to IoT security issues and categorises the most prevalent issues affecting the privacy of data in the network. We also propose some security improvements for IoT and illustrate scenarios of implementing blockchain in IoT.

7. COMPLIANCE WITH ETHICAL STANDARDS

Conflict of Interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies involving human participants or animals performed by any of the authors.

Informed consent Informed consent was obtained from all participants in this study.

ACKNOWLEDGEMENTS

The first author thanks the reviewers for their useful suggestions that improved the presentation of this paper.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] G.R. Carrara, L.M. Burle, D.S.V. Medeiros. Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. *Ann Telecommun*. 2020; vol. 75: pp. 163–174.

[2] D.M.F. Mattos, F. Krief, S.J. Rueda. Blockchain and artificial intelligence for network security. *Ann Telecommun*. 2020; vol. 75: pp. 101–102.

[3] J. Li, X. Liao, N. Puech. Security and privacy in IoT communication. *Ann Telecommun*. 2019; vol. 74: pp. 373–374.

[4] I. Al-Barazanchi, Z.A. Jaaz, H.H. Abbas, H.R. Abdulshaheed. Practical application of IOT and its implications on the existing software. *2020 7th International Conference on Electrical Engineering*. 2020; pp. 10–14.

[5] A. Wu, Y. Zhang, X. Zheng. Efficient and privacy-preserving traceable attribute-based encryption in blockchain. *Ann Telecommun*. 2019; vol. 74: pp. 401–411.

[6] S. Asharaf, S. Adarsh, eds. Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities: Emerging Research and Opportunities. *IGI Global*, 2017.

[7] N. Sabah, A. Sagheer, O. Dawood. Survey: (Blockchain-Based Solution for COVID-19 and Smart Contract Healthcare Certification). *Iraqi J Comput Sci Math*. 2021; pp. 1–8.

[8] Yaga, Dylan, et al. "Blockchain technology overview." arXiv preprint arXiv:1906.11078 (2019).

[9] Ning Shi. A new proof-of-work mechanism for bitcoin. Financial Innovation, 2016; vol. 2, no. (1): p. 31.

[10] Yuanfeng Cai and Dan Zhu. Fraud detections for online businesses: a perspective from blockchain technology. Financial Innovation, 2(1):20, 2016.Cai Y, Zhu D. 2016.

[11] J. Jennifer. Xu. Are blockchains immune to all malicious attacks? *Financial Innovation*, 2016; vol. 2, no. (1): p. 25.

[12] Kshetri, Nir. The global cybercrime industry: economic, institutional and strategic perspectives. Springer Science & Business Media, 2010.

[13] Z. Zheng. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*. 2018; vol. 14: pp. 352–375.

[14] S. Hakak, W.Z. Khan, G.A. Gilkar, M. Imran, N. Guizani. Securing smart cities through blockchain technology: Architecture, requirements, and challenges. *IEEE Network*. 2020; vol. 34, no. (1): pp. 8–14.

[15] B. Bhushan, C. Sahoo, P. Sinha, A. Khamparia. Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. *Wireless Networks*. 2021; vol. 27, no. (1): pp. 55–90.

[16] B.R. Utkurovna. *Blockchain Technologies Characteristics and Advantages JournalNX*; vol. 6, no. (10): pp. 379–383.

[17] S. Demi. Blockchain-oriented Requirements Engineering: A Framework. *2020 IEEE 28th International Requirements Engineering Conference (RE)*. 2020; pp. 428–433.

[18] J. Golosova, A. Romanovs. The advantages and disadvantages of the blockchain technology. *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*. 2018; pp. 1–6.

[19] P. Manoj, Y.B. Kumar, M. Gowtham, D.B. Vishwas, A.V. Ajay. Internet of Things for smart grid applications. *Advances in Smart Grid Power System*. 2021; pp. 159–190.

[20] T.S. Nikoui, A.M. Rahmani, A. Balador, H. Seyyed, H. Javadi. Internet of Things architecture challenges: A systematic review. *International Journal of Communication Systems*. 2021; vol. 34, no. (4): pp. 4678–4678.

[21] M. Javaid, I.H. Khan. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *Journal of Oral Biology and Craniofacial Research*. 2021; vol. 11, no. (2): pp. 209–214.

[22] S. Gopikumar, S. Raja, Y.H. Robinson, V. Shanmuganathan, H. Chang, S. Rho. A method of landfill leachate management using internet of things for sustainable smart city development. *Sustainable Cities and Society*. 2021; vol. 66: pp. 102521–102521.

[23] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, Z. Zou. A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *Journal of Industrial Information Integration*. 2021; vol. 21: pp. 100190–100190.

[24] H. H. Pajooh, M. Rashid, F. Alam, S. Demidenko. Multi-layer blockchain-based security architecture for internet of things. *Sensors*. 2021; vol. 21, no. (3): pp. 772–772.

[25] S. Khan, A.P. Shah, S.S. Chouhan. Utilizing manufacturing variations to design a tri-state flip-flop PUF for IoT security applications. *Analog Integr Circ Sig Process*. 2020; vol. 103: pp. 477–492.

[26] B.D. Deebak, F. Al-Turjman, M. Aloqaily, O. Alfandi. IoT-BSFCAN: A smart context-aware system in IoT-Cloud using mobile-fogging. *Future Generation Computer Systems*. 2020; vol. 109: pp. 368–381.

[27] I.F. Akyildiz, A. Kak. The Internet of Space Things/CubeSats: A ubiquitous cyber-physical system for the connected world. *Computer Networks*. 2019; vol. 150: pp. 134–149.

[28] B. Shang, S. Liu, S. Lu, Y. Yi, W. Shi, L. Liu. A Cross-Layer Optimization Framework for Distributed Computing in IoT Networks. *2020 IEEE/ACM Symposium on Edge Computing (SEC)*. 2020; pp. 440–444.

[29] F. Al-Turjman, J.P. Lemayian. Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview. *Computers & Electrical Engineering*. 2020; vol. 87: pp. 106776–106776.

[30] L. Xiao, X. Wan, X. Lu, Y. Zhang, D. Wu. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security. *IEEE Signal Processing Magazine*. 2018; vol. 35: pp. 41–49.

[31] G. Ayoade, V. Karande, L. Khan, K. Hamlen. Decentralized IoT data management using blockchain and trusted execution environment. *2018 IEEE International Conference on Information Reuse and Integration (IRI)*. 2018; pp. 15–22.

[32] E. Bertino. Data Security and Privacy in the IoT. *In EDBT*. 2016; vol. 2016: pp. 1–3.

[33] A. Al-Hasnawi, L. Lilien. Pushing data privacy control to the edge in IoT using policy enforcement fog module. *Companion Proceedings of the10th International Conference on Utility and Cloud Computing*. 2017; pp. 145–150.

[34] X. Xu, X. Zhao, F. Ruan, J. Zhang, W. Tian, W. Dou, et al. Security and Communication Networks. 2017.

[35] N.M. Kumar, P.K. Mallick. Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science*. 2018; vol. 132: pp. 1815–1823.

[36] O. Novo. Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*. 2018; vol. 5, no. (2): pp. 1184–1195.

[37] M. Swan. Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. *Journal of Sensor and Actuator networks*. 2012; vol. 1, no. (3): pp. 217–253.

[38] D. Mazzei, G. Baldi, G. Fantoni, G. Montelisciani, A. Pitasi, L. Ricci, et al. A Blockchain Tokenizer for Industrial IOT trustless applications. *Future Generation Computer Systems*. 2020; vol. 105: pp. 432–445.

[39] A. Cullen, P. Ferraro, C. King, R. Shorten. On the resilience of dag-based distributed ledgers in iot applications. *IEEE Internet of Things Journal*. 2020; vol. 7, no. (8): pp. 7112–7122.

[40] S. Dewan, L. Singh. (2020). Use of blockchain in designing smart city. Smart and Sustainable Built Environment.