Blockchain-Based Mechanisms to Address IoT Security Issues: A Review

Ochchhav Patel and Hiren Patel

Abstract Internet of things (IoT) is seen as combinations of various communication technologies and embedded equipment such as sensors, micro-controllers, radio-frequency identification, wireless devices, etc., which work as a single unit to achieve a specific task in a smart way, i.e., with less human intervention, and decisions are made automatically. IoT is used in many sectors such as smart home automation, smart grids, smart cities, vehicular networks, etc. Due to easy accessibility and reachability to such devices or networks, there are severe security and privacy issues in IoT. User authentication, access control mechanism, confidentiality and data correctness are a few of the major concerns among them. Though it looks like conventional security concerns, but due to (i) the dynamic nature of IoT, (ii) the resource-scarce nature of the devices and (iii) different standards and communication stacks involved, traditional network security countermeasures may not be applied directly to IoT. In recent years, usage of blockchain technology to address various security issues, specifically data correctness, has opened up a facet for IoT to explore the option of using blockchain in IoT. Researchers have started investigating the same. Primitively, blockchain is a non-editable, decentralized and cryptographically secured ledger that is tolerant against byzantine failure. This nature of blockchain makes it an attractive alternative to address security issues such as data integrity, entity authentication, etc. Also, in an IoT environment, where devices are spread across a vast geographical area, it requires a decentralized validation mechanism that a blockchain provides. In this paper, we intend to make an exhaustive survey of various researches being carried out to secure IoT networks using blockchain technology. We also aim to provide a summarized view for various prospective research directions in IoT which can be addressed by blockchain technology.

O. Patel (✉)
LDRP Institute of Technology and Research, Kadi Sarva Vishwavidyalaya,
Gandhinagar, Gujarat 382015, India
e-mail: ochchhavpatel@gmail.com

H. Patel
Vidush Somany Institute of Technology and Research, Kadi Sarva Vishwavidyalaya,
Gandhinagar, Gujarat 382015, India
e-mail: hbpatel1976@gmail.com

K. Kotecha et al. (eds.), *Data Science and Intelligent Applications*,
Lecture Notes on Data Engineering and Communications Technologies 52,
https://doi.org/10.1007/978-981-15-4474-3_36

Keyword Blockchain · Internet of things · Security · Privacy · Confidentiality

1 Introduction

The Internet of things is the community of physical objects, more than a few devices, buildings, vehicles and other objects which are embedded with electronics, software, sensors, network connectivity, permitting these objects to acquire and interchange data [1]. The Internet of things (IoT) has blasted in recent years, and it is not slackening down any time soon. Gartner forecasts that 20.4 billion connected things will be in use worldwide by 2020, and a report of Gartner (April 10, 2019) predicts that the IoT market will raise to over $3 trillion annually by 2026. The IoT involvement did not stopped to various use cases, but is widely adopted in many other areas such as health care, military, agriculture and smart domain also [2].

IoT finds application in many different fields [3, 4] such as patients remote monitoring, energy consumption control, traffic control, smart parking, inventory management, production chain, transportation and logistics domain and smart health care. Applications of IoT are enormous and user devices in IoT connected with the worldwide Web are keeping on growing, prevention of unauthorized access to IoT data is essential. Since sharing the medical facts of a patient is unethical, the data collected from such environment should be maintained securely. In application of healthcare system, authentication and authorization [5] are key challenges in Internet of things. Authentication and access authorization in IoT, user devices use logging mechanism with username and password. But that kind of mechanisms are often susceptible to attacks. If anybody gets the logging details, then can try to access the healthcare data of a patient purposely and may try to regenerate the medical devices which may downfall the entire system [6]. Smart environment using IoT that making its service easy and comfortable to the intelligence [7] of contained objects. Various projects like smart cities, smart health [8], smart home, smart office, smart shopping, smart mobility and smart transport are running. Butler is a European Union FP7 project [9], its primary persistence about enabling the development of secure and smart life assistant applications in terms of a context and position aware. After the entry of IoT in transportation domain communication, control and data distribution have been improved. Smart components are playing the important role as they carry out the important operations and make work more efficient in heavy loaded vehicles. In transportation domain include personal vehicles, commercial vehicles, trains, UAVs and other equipment. The IoT in smart transportation has rapidly changed the heavy vehicle industries with the help of mobile and connectivity advancements. Geo-fencing that captures the location of devices is most benefitted for transportation industry using IoT [1]. There are three layers [10] in IoT architecture, viz. application layer on the top, network layer in middle and perception layer in the bottom, as shown in Fig. 2. The perception layer plays the role of collection and transmission of data from/to the other layers. The network layer is responsible for steering and conveying the data collected by the perception layer via network technologies such as Wi-Fi, Bluetooth,

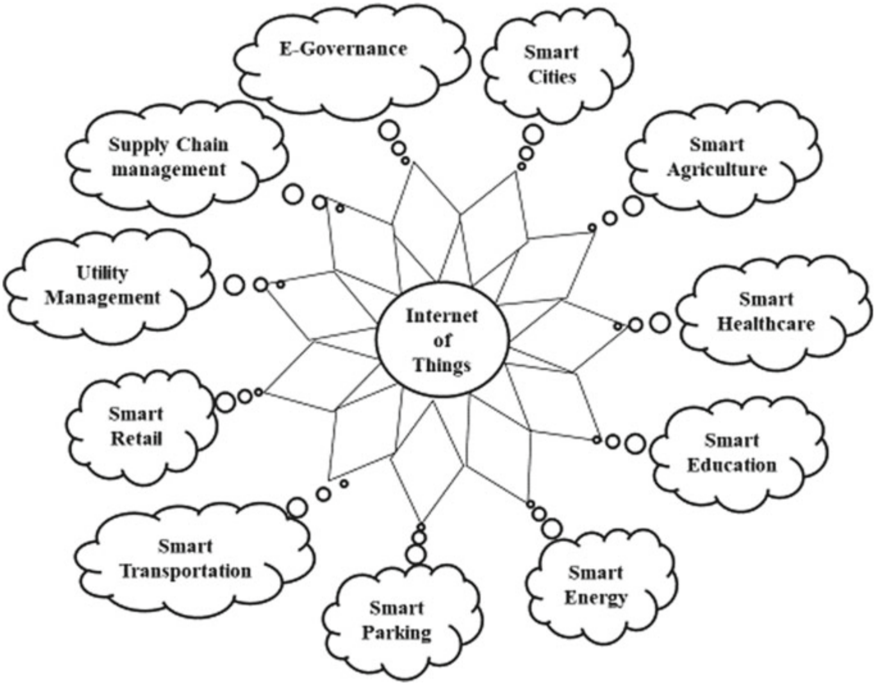

Fig. 1 Internet of things paradigm as a result of the convergence of different visions

3G/LTE and Zigbee. Top layer of the IoT framework is application layer where user interface is created for various application domains as mentioned in Fig. 1.

As mentioned in Fig. 2, the perception layer in IoT architecture mainly consists of sensors and hardware devices so some of the threats are possible by intruder such as spoofing, denial of service (DoS), timing attacks and reply attack. Second layer of the IoT is network layer related to network, communication technologies and corresponding hardware and protocols where traditional security problems of communication networks such as man in middle attack and Sybil attack. Third layer of IoT is the application layer provides interface for kind of services like smart home, smart health care, smart vehicle and smart grids where security threats for the application is dependent on particular domain [8].

Though at first glance, IoT seems to be very attractive options for many of the recent applications, there are few issues yet to be addressed before widely adopting IoT. This paragraph discusses such open issues being faced in IoT. The main issues [1] of IoTs are naming, transport protocol, QoS support, authorization, data integrity, privacy and mobility support. In mobility management, we know several features in IPv6 over IPv4 in mobility application due to efficient routing is achieved by using flexible address and fragmentation at source host and discover the destination path of a maximum of transmission unit. Improved security by using the IPsec protocol

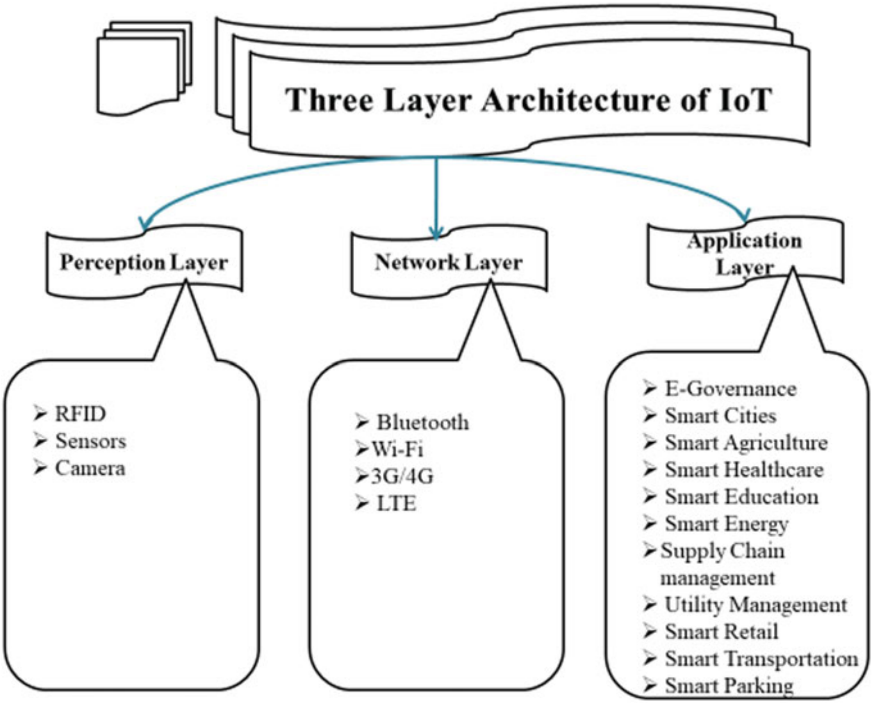

Fig. 2 Three-layer architecture of IoT

achieves better security than IPv4 protocol. Without guarantees in terms of system-level security applicable participants are dubious to adopt IoT solutions on a large scale. The IoT is vulnerable to attacks for several reasons where IoT components spend most of the time unattended so, it is easy to physically attack them. Another reason is the communications are wireless, which makes snooping extremely simple. Most of the IoT components are characterized by low capabilities in terms of both energy as well as computing resources [8]. Main security goals [11] of IoT may include the confidentiality, integrity, availability (CIA), energy efficiency and heterogeneity also. In this section, we mentioned major security challenges to be addressed to turn Internet of things technology into a mainstream and extensively deployed one. In a specific way mentioned here, three key issues [11] requiring innovative approaches that is data confidentiality, privacy and trust.

Due to its nature of immutability, decentralization and avoidance of central authority for decision making, blockchain has become a popular approach for many applications. Few of such applications are as mentioned in Fig. 1. Blockchain used in payment processing and money transfer [12] where blockchain technology provides fast, secure and low-cost universal payment processing services. Use of encrypted distributed ledgers blockchain provides trustful transaction [13] without the need for intermediaries such as correspondent banks. Blockchain provides digital ID that can replace traditional systems with a highly trusted mechanism of managing identities. Blockchain can empower users to have greater control over their own identity using blockchain. Blockchain provides decentralized security and privacy in IoT, involve energy, delay, computational task, etc., that is not suitable for most resource-constrained IoT devices. Blockchain provides secure and private [14] network using mining process for scalability also. Property transfer that is complex and worthy work where blockchain provides important role using of a decentralized application that is smart contract in property transfer process, the entire process, from signing lease agreements to managing cash flow to filing maintenance requests, can be conducted in a secure and transparent manner. In a blockchain-based smart home system, smart home entity can be considered as gateways and main object of homes. Similarly, they all are treated as nodes in the home-based blockchain network. These nodes not only store data but also can be worked as miners in a blockchain-based smart home and perform scalability with security and privacy. IoT issues can be addressed by blockchain architecture and protocols for data access, using smart contracts and a publisher—subscriber [15] mechanism. IoT devices grieve from impersonation and data tampering attacks due to their architectural and computational limitations, which are unable to provide tolerable level of security. Blockchain plays the role and provides unique hardware fingerprints to establish data provenance while Ethereum provides a decentralized digital ledger which is able to withstand data tampering attacks [16].

Asymmetric encryption wants a centralized key administration system, which cannot meet the wishes of an efficient developing IoT system. If the key management system is attacked, a large quantity of IoT units is in all likelihood to be affected. Also, traditional protection methods have a tendency to be expensive for the IoT in terms of strength consumption and processing overhead because sensors are lightweight, of slow processing and of much less memory. Blockchain technology can overcome that kind of problem where proof of work (consensus) calculation is particularly computationally intensive and time-consuming, so IoT devices are restricted and most IoT applications need low latency. Blockchain protocols create significant network traffic flow, which is a catastrophe for the communication of IoT devices.

In IoT, information is added to the network with regular interval means information added to blockchain network where blocks are added and need to be validated in a blockchain network, so mining is required that should be taken into consideration because it demands to high computational power. Alternative matter related to scalability, when the number of nodes increases, the number of transactions increases and the mining and validation process takes lengthier time to be completed [17]. IoT-based Raspbian Pi sensor node can be connected directly to the blockchain as a full node that can validate other transactions or a lite but partial node can only keep a track of its own transactions. The temperature sensor senses the environment and its value is extracted via a Web UI or mobile application. The Web UI or mobile app connected to the blockchain node send the sensor reading to the blockchain environment by smart contract only so Web application or Web app becomes interface between IoT devices and blockchain [18]. This script is organized as follows: Sect. 1 introduces the applications, security threats in IoT and how to address IoT security. Also include introduction about blockchain and issues of IoT addressed by blockchain and challenges of blockchain with IoT when integration performed between these two technologies. Section 2 includes all kind of security issues of IoT and mechanism which have been used to solve IoT security problems using blockchain. Section 3 describes challenges and opportunities of IoT and blockchain domain. Section 4 covered tools and technologies which have been used by existing researcher for their experimentation. Section 5 describes future directions so someone can perform their research in IoT security using blockchain. Section 6 that is final section is concluded with entire paper.

2 Background Theory

A series of blocks is contained in blockchain, in such a way that every new block is cryptographically connected to the previous block so provide tamper proof data storage and transaction. The process of validating and adding transaction to a block and then spreading that block on the blockchain network, to be known by all other the nodes in blockchain is termed as mining [17]. Miner nodes are used to do the mining, and the selection of a node to mine a new block is done based on certain criteria. There are so many types of nodes [18] available in blockchain. Simple node is the most basic, which can only send and receive transactions but cannot store the complete copy of the blockchain. Full node is the node which can maintain a complete copy of the blockchain, but they do not mine a block. A block validation mechanism performed by consensus algorithms such as proof of work in which a miner must perform some predefined work, which is often a mathematical puzzle or challenge which is hard to compute but easy to verify. PoW has the advantage of protecting transactions and blocks from being altered. But one disadvantage of that algorithm is required high computational resources. Another algorithm is proof of stake where there is no mining required by computational solving approach. There are other mechanisms to validate blocks like delegated proof of stake, proof of hold, proof of use, proof of time, proof of minimum aged stake and proof of importance [2].

Blockchain can be permission that is called private or permission—less (public) network. Permission network makes boundary on the consensus contributors and only the chosen trustful nodes have the rights to validate transactions. It does not require a lot of computation to reach a consensus, thus, it is not time and energy consuming. Another type is public blockchain, uses an unlimited number of anonymous nodes, based on the cryptography, each actor can securely communicate. Each node is represented by a pair of private and public keys. Public blockchain is time and energy consuming. We know cloud platform provided various services under the centralized control of one trusted entity, in cloud, it is possible to the single point of failure concerning security and privacy also availability of cloud services. Whereas, blockchain provides a way that all the miner and full nodes in the blockchain network maintains a same copy of the blockchain state and the trust is distributed among all the network nodes. Even though, one of them among blockchain node, want to try to alter data, then system will be reject it, and the blockchain state will be remain untampered [18].

3 Related Work

There are various traits of IoT such as connectivity, heterogeneity, ubiquity, self-organization, mobility, and scalability. Even though, to fulfill full deployment, the security requirements have to be addressed. Confidentiality means to protect data from unauthorized entity, in other words, only the persons can access data who are authorized to access sensitive data. And most important element that is helps to build and develop trust among existing entity in a network. In the IoT context not only users, but also sanctioned objects may access data so important aspects are access control mechanism and object authentication process [8]. Confidentiality should be providing so that the data collected or transmitted are protected and available to authorized users only. As we know collected data from the IoT devices or a sensor should not be transmitted to any other devices without proper encryption applied. Only encoded messages should be delivered to neighboring devices so that malicious entities cannot access the collected data [12]. Confidentiality [19] is very essential, especially in IoT as it makes sure that data and routing information are transferred to only authorize users that can access and alter securely. Hence, speaking forthrightly, the exchanged data within IoT applications should be secure from intermediate and unauthorized entities. The functionality that guarantees that data and directing information have not been changed in transit by a midway or a malicious node is termed as integrity. Hence, any change of exchanged data is imperatively detected.

The functionality in IoT that make sure that entity identity is extremely protected from third party, by defining the rules under which data referring to individual entity may be accessed is termed as privacy. Privacy is the unique considerations required to guard the data of humans from publicity in the IoT environment, in which IoT entities or object can be given a special identification and the capacity to speak autonomously over the Internet. Privacy defines the guidelines under which data referring to individual users may be accessed. Some of the precautions are used to maintain the privacy like set the password, disable universal plug and play and create a separate network or update firm ware [6]. In fitness care, purposes lack of gorgeous mechanism for ensuring privateness of private or sensitive facts has harnessed the adoption of IoT technologies. Health care purposes characterize the most outstanding application field, whereby the lack of fantastic mechanisms for making sure privateness of private or sensitive facts has harnessed the adoption of IoT technologies. In addition, in the IoT vision, a prominent function will be performed via Wi-Fi communication technologies. The ubiquitous adoption of the Wi-Fi medium for replacing facts may additionally pose new issue in time period of privacy violation. In fact, wireless channel will increase the risk of violation due to the remote access capabilities, which potentially expose the gadget to eavesdropping and overlaying attacks. Hence, the privateness represents actual open difficulty that may additionally restrict the improvement of the IoT [11]. Privacy needs to be addressed in the IoT device itself, in storage, during communication and at processing.

The concept of trust is used in a giant range of different contexts and with diverse meanings. Trust is a complex notion about which no consensus exists in the computer and facts science literature, even though its importance has been widely recognized. Mayer, Davis, and Schoorman (1995) define trust as the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective to the ability to monitor or control that other party. Another view of trust by Kimery and McCord (2002) about online transaction is online trust is a customer's willingness and enables to accept an online transaction according to their positive and negative expectations on future online shopping behavior [11]. Trust has been seen and interpreted in many different methods and in distinctive contexts which make it is a very elaborate concept. Because trust is influenced with the aid of many attributes that can be related or no longer to security, authentication, confidentiality, integrity, availability and identity management ought to be regarded a trust principle or have confidence components. Identification consists of providing special identifiers to the entities within the IoT service and correlating these digital identities to real world, legally binding identities. In a cellular network for IoT service, endpoint units are recognized the use of IMSI or IMEI. Networks are identified the use of community codes and country codes where each method of providing identification has various ranges of impenetrable assurance related with it. Blockchains are immutable digital ledger systems implemented in a distributed fashion [20] (i.e., without a central repository) and usually without a central authority. Blockchain applications in multiple use cases and use them as a secure way to create and manage a distributed database and maintain records for digital transactions of all types.

There is a need of architecting the IoT in a reliable manner allowing the ability to automatically adapt to the unexpectedly security break; hence, trust in IoT is very essential for the working. Various solutions in security occur to ensure the different requirements in a various IoT applications. Transport layer security mechanisms or virtual private network used for ensuring confidentiality can be used as an example. To provide integrity, message integrity codes could be used. To secure end-to-end communication between IoT entities, certificate-based authentication could be used. Various IoT issues such as confidentiality, privacy and integrity [18] by configuring and managing IoT devices using blockchain smart contracts are addressed via blockchain. Trust-free distributed architecture [21] is provided by blockchain, where IoT devices are proposed to be configured and managed through Ethereum or other blockchain platform with smart contracts. Bubble of trust [2] has been proposed for IoT devices on decentralized environment to achieve (a) identification, (b) authentication, (c) integrity and (d) availability. Using C++ and Ethereum, it uses blockchain for identification and trust among IoT devices by making use of a concept called bubble. Authors claimed their proposal to be secure, efficient and cost-effective. Authors plan to work upon certain issues such as reducing number of miners and revoking already granted access rights. IoT devices have less memory and low computational capability so it may be easily vulnerable to network attacks so researchers have been introduced integrating technology [19] which is combined with IoT and blockchain. Allocation of the resources in static form to prevent rogue devices accessing from the server, identify trusted and untrusted devices from the network and address DDoS attack also. Researcher claimed new abstract architecture [23] based on service centric networking (SCN) and blockchain provide trust, security and encouragement IoT in a decentralized manner. Proposed decentralized architecture (software stack) [24] based on Blockchain + IPFS and IoT, for retrieving IoT data in a secure manner, peer to peer file storage and abolish the need of centralized IoT data management. Furthermore, researcher enhances their work with hyperledger platform with advanced IoT applications.

4 Challenges and Opportunities

There are various drawbacks that the researchers feel about the IoT security domain such as client privacy, denial of service, secure communication and double spending. It is essential to the information and data of individuals from the exposure in the IoT environment, which makes the privacy in IoT a very consideration. There are times when any particular service is not available, this situation whenever arises, is termed as denial of service [21]. There could be multiple reasons for such inaccessibility, but on a higher probable cause, it refers in most cases to the infrastructure that cannot manage due to capacity overload. There are three types of DOS attacks; (1) application layer attack, (2) protocol and (3) volume-based attack. The biggest challenge in an IoT is the secure communication using symmetric and asymmetric encryption. Public and private keys are complimentary to each other and both are asymmetric keys. Any message that is encrypted by a public key will be decrypted by a private key. Same follows the other way around. For generating a shared key using asymmetric elliptic curve keys [19] is done using elliptical curve Diffie–Hellman.

As there has been an over-exhaust in the recent past, with the improvement, development of science and accessibility of the wireless devices has increased. Cloud computing seems to be the possible solution for such large number of wireless devices connected to Internet, but security challenges could not be satisfied by it. For private and sensitive data in an IoT will continue to face security problems. Thus, the need for a completely decentralized peer to peer and secure technology as a blockchain can have the sustainability to overcome these problems [15]. Due to the architectural and computational limitations, many IoT devices suffer from data tampering and impersonation attacks. BlockPro have been implemented by many researchers which is a blockchain-based system for data provenance and data integrity [16].

5 Tools and Technologies

Though blockchain has the potential to evolve various industries, like health care, logistics and supply chain, insurance, financial and many more reputed companies are also adopting blockchain, but the blockchain is well known for cryptocurrencies such as Bitcoin and Ethereum. There are multiple networks for blockchain such as Ethereum, Hyperledger Fabric and Bitcoin [2]. Ether is the cryptocurrency provided by Ethereum which is a public blockchain. Ethereum virtual machine is the operating system used in Ether where smart contacts are executed. Ethereum takes only 14s to validate a block in a network, whereas the Bitcoin takes 10 min. Ethash is the consensus mechanism for Ehtereum for block validation mechanism. Hyperledger is the other option, which is an open-source blockchain created by the Linux Foundation, more specifically by IBM and it does not provide a cryptocurrency. There are so many blockchain tools available to create blockchain [25] environment such as remix IDE, solc, geth, embark, ganache, baas, mist and metamask. One of the easiest and browser-based tools to use for the creation and deployment of smart contracts is the remix. For writing, debugging, testing and deploying smart contracts is the solidity language. It is syntax is a loosely typed programming language and has syntax similar to European Computer Manufacturer's Association (ECMA) script. Though one needs something to convert solidity script into a format readable by the EVM, this purpose is fulfilled by solidity compiler. Solidity compiler can be divided into two parts one is solc coded in C++ and second is solc-js that uses Emscripten for cross-compiling from solc C++ code to JS. In Go Programming, Geth is an Ethereum client used for Ethereum client. Logically, Geth [25] is a program which works as a node for the Ethereum platform. There is a development framework for Ethereum-based dApps. It is used for give permission to the developers to develop and deploy dApps on decentralized technology. It has the eligibility to permit you to create smart contracts which can be made available in Javascript code. It also provides with the application of migration if the application has multiple contracts. With the Javascript developers and the support of the test-driven development of smart contracts can handle contracts on different blockchains like testnet, live network and private net.

6 Future Directions

The applications of IoT and its importance in daily life in increasing to a very large extent, and hence it should require secure communication among devices in a network. The researchers working in this wide field have proposed the concept bubble of trust [2] where the virtual zones which are proven secured are created where devices can communicate in a way that is completely secure. The ultimate purpose is to enhance the work to establish a revocation mechanism for the devices that are compromised. The design protocol is the one that aims the optimization of the miner's number in an already defined system as well as how the miners that are selected can be placed. Credibility verification method for IoT devices have been implemented by the researchers and are getting the advantage in the aspects of the storage space and response time. It has also been mentioned by them that there is a lot of work in the near future for IoT environment and in determining how to choose the number of blockchain structure node (BCS) [26]. Not all researchers have implemented service centric networking (SCN) to provide reliable connectivity and the global scalability in IoT network. It is considered as a combined amalgamation of SCN and blockchain to empower the IoT [23]. A new combination of the architecture of OSCAR [27] and ACE [28] is the authorization framework to provide the end-to-end solution for the secure authorized access to IoT resources. Their enhancement is based upon the updation of private Ethereum blockchain network to use the PoS version of the ledger.

7 Conclusion

With the advancement in technology to develop smart applications such as smart cities, smart transportation, smart health care, etc., the Internet of things (IoT) has become a topic of buzz as it is one of the basic building blocks behind it. IoT equipments are often used in a coarse way as they are to be installed in any territory with/without observations. Unobserved devices are prone to fall in security breaches which may cause severe damages. Hence, it is of utmost importance to understand all such security problems and propose solutions for the same. Some of the network security issues can be addressed through traditional cryptographic primitives, however, due to the distinct nature of IoT, few security concerns are to be addressed in a diverse way. One of such solution provider to security predicament is blockchain technology. Due to a few attributes such as non-editability, transparency, avoidance of central arbiter and distributed environment, researchers have commenced exploring the use of blockchain technology to find out the solutions to IoT security problems. In this research, we have studied various existing mechanisms proposed in recent times with their detail analysis. We have discussed the fundamental terminologies related to blockchain technology along with all the challenges and opportunities. We also have investigated various tools and technologies pertaining to blockchain along with future research work which can be carried out in this domain. In the upcoming time, we wish to propose a novel security mechanism for IoT using blockchain technology.

References

1. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. Comput Netw 54(15):2787–2805
2. Hammi MT, Hammi B, Bellot P, Serhrouchni A Bubbles of trust: a decentralized blockchain-based authentication system for IoT. Comput Secur 78:126–142

3. Yuan R, Shumin L, Baogang Y (2007) Value chain oriented RFID system framework and enterprise application. Beijing: Sci (2007)
4. METRO Group Future Store Initiative. http://www.futurestore.org/
5. Vilamovska AM, Hattziandreu E, Schindler R, Van Oranje C, De Vries H, Krapelse J (2009) RFID application in healthcare—scoping and identifying areas for RFID deployment in healthcare delivery, RAND Eur
6. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I (2012) Internet of things: vision, applications and research challenges. Ad Hoc netw 10(7):1497–1516
7. SENSEI FP7 Project, Scenario Portfolio, User and Context Requirements, Deliverable. http://www.sensei-project.eu/
8. Shantha JR (2016) A neoteric authentication scheme for Iot healthcare system. https://doi.org/10.5281/zenodo.192911
9. BUTLER Project. http://www.iot-butler.eu
10. Shin H, Lee HK, Cha HY, Heo SW, Kim H (2019) IoT security issues and light weight block cipher. In: International conference on artificial intelligence in information and communication (ICAIIC), IEEE, pp 381–384
11. Nabil D, Tandjaoui D, Romdhani I, Medjek F (2018) Trust management in internet of things. https://doi.org/10.4018/978-1-5225-5736-4.ch007
12. https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx
13. Guo, Y, Liang, C (2016) Blockchain application and outlook in the banking industry. Finan Innov 2(1):24
14. Yaga, D, Mell, P, Roby, N, Scarfone, K (2018) Blockchain technology overview (No. NIST Internal or Interagency Report (NISTIR) 8202 (Draft)), National Institute of Standards and Technology
15. Rifi, N, Rachkidi, E, Agoulmine, N, Taher, NC (2017) Towards using blockchain technology for IoT data access protection. In: 2017 IEEE 17th international conference on ubiquitous wireless broadband (ICUWB), IEEE, pp 1–5
16. Javaid, U, Aman, MN, Sikdar B (2018) BlockPro.: blockchain based data provenance and integrity for secure IoT environments. In: Proceedings of the 1st workshop on blockchain-enabled networked sensor systems, ACM, pp 13–18
17. Mining in Bitcoin. Available at: https://en.bitcoin.it/wiki/Mining/
18. Makhdoom, I, Abolhasan, M, Abbas H, Ni W (2019) Blockchain's adoption in IoT: the challenges, and a way forward. J Netw Comput Appl 125:251–279
19. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE international conference on pervasive computing and communications workshops, PerCom workshops, IEEE, pp 618–623
20. Zheng Z, Xie S, Dai HN, Wang H (2016) Blockchain challenges and opportunities: a survey. Work Pap
21. https://www.cloudflare.com/en-in/learning/ddos/what-is-a-ddos-attack/
22. Ming Z, Yang S, Li Q, Wang D, Xu M, Xu K Blockcloud: empowering IoT through a service-centric blockchain. Blockcloud Technical White Paper
23. Ali MS, Dolui K, Antonelli F (2017) IoT data privacy via blockchains and IPFS. In: Proceedings of the seventh international conference on the internet of things, ACM, pp 14
24. https://hackernoon.com/top-12-blockchain-development-tools-to-build-blockchain-ecosystem-371a1b587248
25. Qu C, Tao M, Zhang J, Hong X, Yuan R (2018) Blockchain based credibility verification method for IoT entities. Secur Commun Netw
26. Vučinić M, Tourancheau B, Rousseau F, Duda A, Damon L, Guizzetti R (2015) OSCAR: object security architecture for the internet of things. Ad Hoc Netw 32:3–16

27. Seitz L, Selander G, Wahlstroem E, Erdtman S, Tschofenig H (2017) Authentication and authorization for constrained environments (ACE). Int Eng Task Force Int Draft Draft Ietf Aceoauth Authz 07 work Prog. Available at: https://datatracker.ietf.org/doc/html/draft-ietf-ace-oauth-authz-07
28. Alphand O, Amoretti M, Claeys T, Dall'Asta S, Duda A, Ferrari G, Zanichelli F (2017) IoT Chain: a blockchain security architecture for the internet of things. In: IEEE wireless communications and networking conference (WCNC), IEEE, pp 1–6