A Study on Leveraging Blockchain Technology for IoT Security Enhancement

Syeda Mariam Muzammal[1], and Raja Kumar Murugesan[2]

School of Computing & IT, Taylor's University, Subang Jaya, Malaysia
[1]syedamariammuzammal@sd.taylors.edu.my, [2]rajakumar.murugesan@taylors.edu.my

***Abstract*—In the rapidly growing digital and technological world, Internet of Things (IoT) is becoming very popular and widely implemented. As more and more IoT devices are deployed in an uncontrolled, complex and often hostile environment, securing the IoT devices, systems and data exchange presents numerous unique challenges. With data sensitive IoT applications, there is an utmost need to protect and explore user privacy, access control, third party involvement, and Machine-to-Machine (M2M) information exchange in order to avoid critical security breach and cyberattacks. Most of the security and privacy issues of the interconnected heterogeneous resource constrained smart IoT devices are unable to be solved efficiently by traditional security practices. On the other hand, Blockchain technology is well-thought-out as emerging and revolutionary concept, initiated from cryptocurrency, and now making way to enhance various scenarios in digital paradigm, mainly due to its decentralized nature and transparency. This paper reviews the adoption of IoT in various fields and its applications to automate and improve living conditions, along with security and privacy risks arising from organization and functioning of different IoT components. Moreover, the study is specifically based on how effectively the Blockchain technology can be leveraged for strengthening IoT security and privacy implications, and possible limitations of embedding Blockchain with IoT framework.**

Keywords—Internet of Things, Blockchain, IoT Security, Privacy

I. INTRODUCTION

Smart devices are ubiquitous in today's world. The emergence of IoT paradigm has given rise to the rapid escalation in use of smart heterogeneous interconnected devices and applications. The IoT is a network of swiftly growing complexity, whereas blockchain has been activated for a substantial impact on IoT by its decentralized nature and other features of security enhancement and empowerment for accommodating a number of devices in the IoT paradigm. Both have the antagonistic capabilities to transform concepts into realities and providing innovative opportunities to develop advanced and secure applications.

With its wide adoption in different industries, like supply chain management, agriculture, farming, transportation, insurance, and health, IoT has a number of well-known security defects that have given rise to recent attacks [1]. The enhanced and autonomous functionalities lead to exposure of sensitive data, in M2M communications, to malicious activities. For example, the personal data communicated through wearables can be delivered to undesired sniffing nodes that may cause intense privacy breach for an individual [2].

For this most commonly implemented infrastructure, efficient and reliable techniques for security and privacy have become an obligatory issue for the wide adoption of IoT technology. Conversely, Blockchain, based on decentralized and distributed ledger technology is influencing IoT applications for faster adoption by enterprises towards digitized and secure smart world. Extensive research work is going on for the exploitation of Blockchain for IoT in different industries and many big companies, like IBM, have already taken on the challenges.

This paper presents a study and discussion on IoT applications, security and privacy requirements according to its characteristics and how effectively the emerging blockchain technology can be viewed in IoT context with respect to cybersecurity needs, privacy-preservation, secure data transmission and connection between IoT interconnected and resources constrained devices. Rest of the paper is structured into five sections. Section 2 presents the background and theoretical groundwork for understanding of IoT and its applications, IoT security and privacy implications, and a brief introduction to blockchain technology. Section 3 describes how the combination of blockchain and IoT can be beneficial in IoT use-cases along with the limitations that IoT poses in implementation of blockchain solutions. Section 4 presents the related work as done by the researchers in said aspect. Section 5 elaborates the discussion and open issues, and finally section 6 concludes the study.

II. BACKGROUND

A. IoT and IoT Applications

IoT is the interconnection of physical devices, forming a network of smart things that communicate and exchange data with one another to reduce human exertions, improve efficiency of systems and overall economic benefits. Many industries are adopting IoT solutions, such as smart cities, connected cars, poultry and farming, supply chain, healthcare, surveillance systems, energy management, transportation, agriculture, insurance, retail, logistics and various others.

In an IoT system, a plethora of devices can be connected to the internet based on the notions of IoT, making possible the implementation of routine tasks with M2M communication. The basic components of IoT system include the IoT devices to collect data (for example, sensors, antenna, and microcontroller), IoT hub or gateway to collate and transfer data, and the user interface or back-end systems.

B. IoT Security and Privacy Implications

The general acceptance and mass adoption of IoT is based on assurance of privacy and security, as they collect vast amounts of sensitive information related to users'

978-1-5386-7167-2/18/$31.00 ©2018 IEEE

identity, health, environment, location, operations, routine tasks and activities, and certain crucial data related to individuals and industries as well as militaries. Fig. 1 shows a generic taxonomy of IoT security and privacy. Various security and privacy concerns, related to devices, data, networks and users, in functional and infrastructural aspects of IoT need to be considered for enhanced solutions. Some of the substantial challenges related to security and privacy for interconnected IoT devices, applications and networks are briefly described as below:

Lack of Standardization: The use of several different standards for development and deployment of IoT applications, leads to incompatibility and unexpected incidents [3]. For example, sometimes system administrators are unable to monitor and control IoT devices. Similarly, sufficient access control mechanisms are not incorporated for some IoT devices that may cause privacy breach.

Device Identification: IoT devices need to have secure identities and ownership, which are currently not provided or just provided by the device manufacturers.

Device updates: For ongoing maintenance and security, device firmware needs to be updated with regular intervals, thus require implementation of a scheme for only authenticated updating of devices.

Data Sharing: The interconnected IoT devices share a large amount of data with each other and with external sources that require proper authorization and authentication mechanism for secure data interchange and command consent. Moreover, to preserve the privacy, there should be proper user consent mechanism to keep the right of individuals to share their information. For example, in healthcare IoT using the patients' data without their permission.

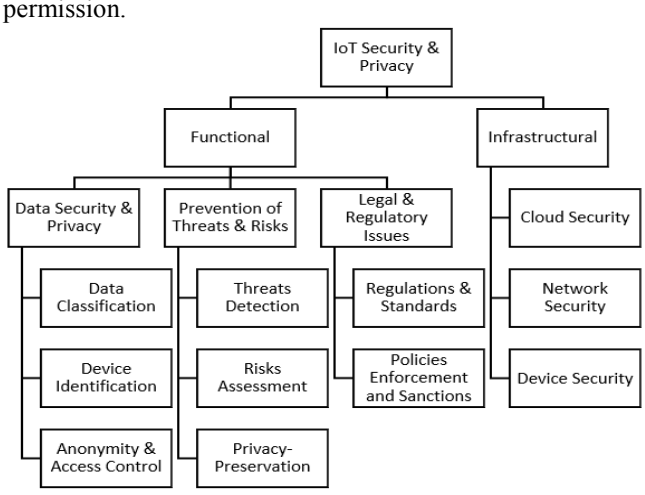

Fig. 1. Taxonomy of IoT Security and Privacy

Anonymity and Access Control: Privacy-preservation can only be achieved with proper embedding of data and user anonymity with access control only by authenticated parties. In IoT, usage of personal data by outsourced parties and monitoring of individual's data as in healthcare applications may cause privacy breach.

Logging: For the command issuance and implementation, data transactions and revocations need to be logged and monitored to resolve any possible disputes.

Policy sharing and validation: Another perspective for secure IoT relies on policy sharing and validation that can contribute to access control and authorization. Moreover, lack of applicable policies and sanctions enforcement to devices may lead to data leaks, and privacy and security breaches.

Centralization in IoT: The current IoT infrastructure relies on a centralized mechanism, a hub or gateway for processing that may be through a cloud or a third-party service provider. This leads to dissemination of information to Trusted Third Party (TTP) by relying on their security and privacy-preservation mechanisms. The low powered, resource constrained IoT devices and platform have unique security requirements related to centralization and weak communication channels. Hence, need a dedicated scheme to embed security in IoT. Another major concern in centralized IoT infrastructure is the availability. Since, IoT networks are integrated with a platform that leads to a single point of vulnerability.

Overlapping IoT Security and Privacy Challenges with other technologies: Since the IoT platform is based on cloud, which also IoT security concerns to cloud computing. Additionally, for the interconnection and wireless networks, the IoT threats overlap with networks security. For example, unsecure communications with data exposure and exchange over public Wi-Fi/Internet. However, there have been specific and critical challenges that are restricted to IoT infrastructure.

Distributed Denial of Service (DDoS) Attack: The IoT security concerns reached the hype in September 2016 when Mirai botnet attack caused immense disruption by DDoS outbreak against a major DNS provider, Dyn. The shot was made possible and successful through security cameras [4] [5], using dictionary password with direct access for internet connected devices [1]. Similarly, in the later kinds of Mirai botnet attack, IP spoofing attacks were launched. Other such attacks include the turning of Smart TVs into secret listening devices by CIA [6], accident by remotely controlling a jeep [7], destruction of nuclear centrifuges of Iran by turning it out of control through Stuxnet virus [8].

Hence, the above-mentioned security and privacy implications of IoT and the cyber attempts emphasize the need for the enhancement and an upgraded security and privacy-preserving solutions for IoT.

C. Blockchain Innovation

A blockchain is basically a growing list of records, called blocks, which are cryptographically linked together, forming a chain of blocks. Blockchain technology is considered as a vigorous and robust solution for cybersecurity and privacy preservation in various technological scenarios, especially in IoT. The technology itself is said to be secure by design for its decentralized nature [9]. In a blockchain model, there is no need for an intermediate or third party to store data, instead the data is stored in a distributed manner in which each node holds an identical set of information. Hence, there is no single point of failure. If security breach is occurred at one device or node, system rejects its activities, hence securing rest of the network [10]. Additionally, multi-signature mechanism for authentication and verification, and cryptographic linkage of blocks provides further protection to the data in nodes and strengthens the

blockchain to defend malicious attempts. The privacy-preservation in blockchain can be guaranteed by keeping the transactions anonymous, depending on blockchain platform being used and the underlying application design.

Moreover, blockchains can be either permissioned or permissionless [11]. Hence, can be accommodated according to the requirements of the IoT use case for effective enhancement of security and privacy. The permissioned blockchains are private and restricted with a closed group of only known participants to which access is granted by some authority [12]. Whereas, permissionless blockchains are open platform and public in nature in the aspect there is no known participants, and anyone is allowed to join or leave the blockchain anytime [9] [13].

III. Convergence of Blockchain and IoT to Overcome Certain Challenges

Blockchain is considered to possess the potential of providing enactment of anonymity, trust, authentication, integrity and operative contracts between involved participants or groups, without the need of an intermediate party to be trusted. Any corporate or private sector organization with a system and IoT devices can enhance productivity and eradicate single points of fiasco in systems by objectifying this innovation and using either permissioned or permission less blockchains or integration of both [11].

A. Blockchain Characteristics to Improve IoT

Blockchain possesses a number of outstanding characteristics that make it suitable for addressing shortcomings of IoT. IBM has mentioned three key benefits of Blockchain for IoT including trust building, cost reduction, and transactions acceleration [14]. Others include, decentralization, immutability, anonymity, authentication, verification, credibility, trust building, and overall security from numerous malicious attacks.

B. Use Cases of Blockchain-based IoT

Some of the major use cases of Blockchain-based solutions for IoT applications are discussed below.

Supply chain: In supply chain IoT, achieving transparency is the key issue. Blockchain-based solution can provide visibility, optimization, petition, as well as proper access control for data sharing among the participants involved. The integrity, availability and reliability of real-time data access will increase the efficiency of supply chain management.

Vehicular IoT: One of the most beneficial application of blockchain-based IoT solutions is automotive industry by providing real-time data access and execution of transactions among big auto companies, manufacturers, partners, service providers, insurance, financing authorities, regulators and customers. On-the-go decisions, services and payments are made easier through blockchain integration. For example, to assist manufacturing a single car, Toyota has taken an initiative for the tracking of vehicular parts that are transported throughout the globe via factories and suppliers.

Energy Management and Smart Grid: With the integration of blockchain and IoT in energy industry, there has been tremendous increase in the efficiency of smart grids and energy distribution, along with the monitoring and control of dissemination of resources. For example, it can be made possible for the excess energy release from the solar panel on a roof-top, to other users who need it, along with record and payment without any security and privacy breach. Similarly, blockchain-based mesh networks of IoT devices can be deployed to monitor energy grids for fault tolerance and fixing an arising malfunction as early as possible.

Healthcare: One of the blockchain-based IoT solution in healthcare is the self or remote monitoring of patient's data through wearables or other smart devices. The security of patient's data and privacy is ensured by storing data in a distributed ledger and defining smart rules of access in blockchain. The use of Blockchain is also significant in pharmaceutical supply chains.

Other applications: Apart from the mentioned above, there are certainly tremendous unknown applications of blockchain-based IoT, providing evidence that management and security of IoT devices and privacy-preserving data flow in networks can be improved by integration of blockchain technology. Additionally, it empowers the access control of data and services and data exchange among involved parties. Since, blockchain is born to be a technology for cryptocurrency, hence can facilitate for secure payment services in accordance with operations and flow of data, while maintaining the anonymity.

IV. Related Work

The potential of Blockchain's integration in IoT is being evaluated through variable measures envisioned to strengthen security and privacy. A number of initiatives have been made by industries and organizations for the development of efficient IoT solutions based on blockchain to enhance production with satisfactory consumer's experience. A group of highly reputed companies was formed in January 2017 for setting security standards of IoT applications using blockchain [17]. Similarly, several companies are heading towards integrating blockchain into their businesses. For example, Provenance has started building a traceability data system using blockchain for tracking of materials and goods, which is auditable and open to public, providing transparency of products [18].

Similarly, Filament is working on integration of blockchain technology in industrial Internet of things (IIoT) for secure execution of transactions making connections of devices independent of central authority [19]. Moreover, via giant cloud infrastructure, IBM is providing blockchain services for supply chain items tracking [20]. In addition to the top high-tech companies, researchers are also working hard to explore blockchain-based solutions for IoT, to enhance efficiency via decentralized interconnection, and specifically security and privacy of the overall system and its components. For example, in logistics and supply chain management system [21]–[24] and Smart grid and energy management [25], [26]. Most of the experts are interested in improving

TABLE I. SUMMARY OF SHORTCOMINGS OF IOT AND BLOCKCHAIN SOLUTIONS

Shortcomings of IoT		Blockchain Solutions
High costs	- Increased cost with scalability and addition of new IoT devices - Need for large servers and networking equipment - Maintenance and infrastructure cost	- No third party needed - Autonomous and distributed storage - Non-central and dispersed control guarantees robustness and scalability
Single point of failure	- Possibility of bottleneck - One malicious node can disrupt the entire network - IoT small devices are susceptible to DDoS attacks, data theft and remote hijacking.	- Interlocked devices - Data breach on/from one device, that device is thrown out of Blockchain - Utilizing resources of all participating nodes and eliminating one-to-many and many-to one traffic flows
Susceptibility to manipulation	- Mismanagement of data - Manipulation of findings in a particular direction	- Trackability - Immutability: data once entered or once a transaction is occurred, cannot be altered or deleted
Downtime & Unavailability	- Since, current infrastructure of IoT is mostly dependent on cloud, hence possibility of servers down or cooling	- Transactions are on a number of devices to hold identical information - A faulty node can join in or leave the system anytime
Unsecure Communication	- Communication is through third party or cloud	- Leverage smart contracts for secure communication - Message exchanges between occurs same as financial transaction in bitcoin
Privacy Breach	- Personally identifiable information (PII) can be exposed, for example, through profiling	- Anonymity of personal data by cryptographic linkage of nodes - Confidentiality is maintained similar to securing identity and balance information in bitcoin
Authentication	- Relies on trusted third party (TTP)	- Cryptographically signed transactions - Verification of digital signatures - Trust building - Eliminating Man-in-the-middle and replay attack
Credibility	- No authorization and data integrity mechanism	- Collective verification via consensus mechanisms - Tamper resistance – each node holds identical copies of data - Can check on malicious nodes

smart home IoT devices and application, to improve human experience and facilitation [27]–[31]. Others have proposed enhanced blockchain-based solutions in various areas, like agriculture [32] and social networks (Social IoT)[33]. Further work comprises of blockchain-based solutions for secure IoT devices interconnection [34], ownership of IoT devices [35], authentication [36], networks [37]–[40], servers overloading [41] and data storage [42]. A lot of work is still ongoing in exploring the potential of blockchain-based solutions for improving IoT applications, devices and the security and privacy implications [43] [44] [45]. To overcome the blockchain overhead, [16] proposed an IoT compatible architecture based on blockchain, while preserving its benefits of security and privacy. Similarly, to support the continuous synchronization and overcome the challenges of third party and client server model, [46] proposed blockchain-based platform using Ethereum for controlling and configuring IoT devices.

Currently, the idea of blockchain-based IoT solutions is just at preliminary stage. It is evident that there is a possibility of a blockchain based infrastructure, for IoT, built upon distributed ledger technology enabling smart contracts, like Ethereum and Hyperledger. However, most of the work is focused on Ethereum blockchain since it is permissionless and lightweight, well suited for the requirements of IoT. Though a lot of research work and initiatives are undergoing in this area, till now blockchain has not been widely adopted and extensively used, which shows that it has not been really tested effectively to evaluate its real potential.

V. DISCUSSION

There are a number of privacy and security violation causes in a non-blockchain infrastructure that are not applicable to blockchain world [9]. Organizations store a huge volume of information including personal and confidential data for analysis and to reveal novelties in their businesses without considering the security and privacy impacts. Moreover, the collection, storing, processing and sharing of data is handed over to the third parties, and hence may involve cloud service providers (CSPs), relying on their security standards, and giving rise to potential security and privacy issues. A summarized picture for the security and privacy-preserving features that blockchain can support for IoT is depicted in Table 1.

A captivating characteristic of blockchain is that the personal data can only be viewed with permission from the individual and it cannot be stored for later retrieval. The cryptographic technique is used to store proof of identity hence, breaking it is almost impossible [47], providing a strong privacy protection mechanism. Moreover, cryptographic identity and access control systems can be helpful in avoiding IP Spoofing attacks. Furthermore, a robust application of blockchain is considered to be the sheltered storage with digitally signed messages and documents transmission. Such applications, in order to validate assets and individual's identity, are being built and verified in shipping, finance, insurance, and especially in automated IoT scenarios.

By using blockchain's decentralized, autonomous and trustless nature, a number of key security and privacy

challenges related to the centralized model of cloud can be addressed. Moreover, if IoT devices are placed just at a close distance to each other, still connections and communications between them go through the internet and TTP [48]. Likewise, centralized models are expensive and problematic to manage when employed to heterogeneous scenarios like IoT, hence leading to the adoption and effectiveness of a blockchain-based decentralized approach. The exponential increase in network size, scalability issue of IoT, can be made more secure by consensus driven structure of blockchain. Since, data in blockchain is dispersed around several devices or nodes that are interlocked together to form a chain - blockchain; an attacker can only be successful, if manage to hack more than 50% of the blockchain network. It is also worth noting that, while bitcoin is the application that utilized blockchain structure for cryptocurrency, has had a perception among public about hacking attempts [15]. However, it has been reported that there is no successful hacking on bitcoin transactions till now, rather it occurred to the systems that were holding and storing bitcoin private keys [49][9].

The blockchain for IoT is being proved and worked upon by researchers by applying core blockchain approaches and components to multiple industries, sectors, applications and use-cases of IoT infrastructure. Through the general ideas of IoT security and privacy perceptions with reference to the current model and blockchain-based solutions (as depicted in Table 1), it can be inferred that traditional security methods do not fit the needs of IoT resources-constrained devices and infrastructure. IoT requires privacy and security protection that is light, scalable, and distributed that Blockchain has the potential to provide [13]. However, it is not light, rather computational intensive, hence require adaptations and optimizations to meet the needs of IoT privacy and security.

Accountability of the individual roles in transactions is ensured by blockchain, thus avoiding disputes. Since, blockchain is immutable, cannot be altered or deleted, hence denying the possibility of devices connecting to a network by masquerading and forging signatures. Specifically, device identification can be managed just like the cryptocurrency model that provides ownership of bitcoins; the workout can be enhanced for IoT devices and users. The choice of permissioned and permissionless blockchain depends on various types and number of authorizing participants with varying credentials as well as the nature and importance of assets being exchanged or transferred.

From the above discussion, it is apparent that blockchain may prove to be a nightmare for cybercriminals, data manipulators and others who mishandle personal data and devices. While blockchain is foreseen to address various aspects of security and privacy, the most promising is the control of personal data by individual itself. For example, after the government agency provides a digitally signed copy of a document (e.g., driving license, ownership documents of vehicle, house, land and other assets), and add it to blockchain, it is then immutable and cannot be accessed or modified [50]. Additionally, it should be noted that blockchain currently is in its emerging state. The number of applications based on DLT and blockchain are evolving in order to adequately evaluate the superiority of this technology to the current systems in defending against various cyberattacks, threats and risks. However, the architecture and structure of blockchain infrastructure is promising to be incorporated for the enhancement of IoT smart applications.

VI. Conclusions

Keeping in view the sensitivity of smart devices' functionality, and data they collect, generate and process, IoT solutions should address the potential security and privacy concerns. It is noted that IoT security and privacy concepts periodically change with the change in trends and technology, and moreover with the adapting industry or use case. The "Blockchain" not only enables the movement of money but can also be used to secure transfer of information and allocate resources between devices, enabling the use of Blockchain as a service for IoT. The connected world can usefully include Blockchain technology as a layer for which more and more devices (wearables, sensors, IoTs, smartphones, tablets, laptops, homes, cars, and smart cities) can benefit from the advanced characteristics. This study presented the shortcomings of IoT and characteristics of Blockchain that can be valuable to achieve desirable security and privacy in IoT infrastructure and applications. It has been discussed that blockchain presents many promising opportunities for the future of IoT. Challenges, however, remain, as consensus models and computational costs of transaction verification. Nevertheless, it is still in the early stages of developing blockchains, and these obstacles will eventually be overcome, opening the way towards many possibilities and changing concepts into realities.

References

[1] P. Fremantle, B. Aziz, and T. Kirkham, "Enhancing IoT Security and Privacy with Distributed Ledgers - A Position Paper," *Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, no. April, pp. 344–349, 2017.

[2] R. K. Lomotey, "Enhancing Privacy in Wearable IoT through a Provenance Architecture," 2018.

[3] C. Vorakulpipat, E. Rattanalerdnusorn, P. Thaenkaew, and H. Dang Hai, "Recent challenges, trends, and concerns related to IoT security: An evolutionary study," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2018–Febru, pp. 405–410, 2018.

[4] C. Lee, J. Jo, J. Lee, D. An, and J. Cho, *Internet of Things – ICIOT 2018*, vol. 10972. Springer International Publishing, 2018.

[5] C. Lee, J. Jo, J. Lee, D. An, and J. Cho, *A Blockchain-Based Decentralized Security Architecture for IoT - Internet of Things – ICIOT 2018*, vol. 10972. Springer International Publishing, 2018.

[6] "WikiLeaks hits CIA secrecy on software spying - The Boston Globe." [Online]. Available: https://www.bostonglobe.com /business/2017/03/08/wikileaks-hits-cia-secrecy-software- spying /EQdLVwseMu70HEYlZcowOO/story.html. [Accessed: 31-Jul-2018].

[7] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It | WIRED." [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed: 31-Jul-2018].

[8] Michael B Kelley, "Stuxnet Was Far More Dangerous Than Previous Thought - Business Insider." [Online]. Available: https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11/?IR=T. [Accessed: 31-Jul-2018].

[9] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecomm. Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[10] R. Kestenbaum, "Why Bitcoin Is Important For Your Business." [Online]. Available: https://www.forbes.com/sites/richardkestenbaum/2017/03/14/ why -

bitcoin-is-important-for-your-business/#1e0bcaf641b5. [Accessed: 31-Jul-2018].

[11] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[12] O. Bussmann, "A public or private blockchain? New Ethereum project could mean both | American Banker." [Online]. Available: https://www.americanbanker.com/opinion/a-public-or-private-blockchain-new-ethereum-project-could-mean-both. [Accessed: 31-Jul-2018].

[13] E. F. Jesus, V. R. L. Chicarino, C. V. N. De Albuquerque, and A. A. D. A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," *Secur. Commun. Networks*, vol. 2018, 2018.

[14] iscoop, "Blockchain and the Internet of Things: the IoT blockchain opportunity and challenge," vol. 3.

[15] N. Lohade, "Dubai Aims to Be a City Built on Blockchain - WSJ." [Online].Available: https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080.[Accessed:31-Jul2018].

[16] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and Solutions," Aug. 2016.

[17] "Companies forge cooperative to explore blockchain-based IoT security | CIO Dive."[Online].Available: https://www.ciodive.com/news/companies-forge-cooperative-to-explore-blockchain-based-iot-security/435007/. [Accessed: 02-Aug-2018].

[18] "Technology | Provenance." [Online]. Available: https://www.provenance.org/technology. [Accessed: 31-Jul-2018].

[19] "Enabling the Future of IoT Filament." [Online]. Available: https://filament.com/. [Accessed: 31-Jul-2018].

[20] "Blockchain for Supply Chain - IBM Blockchain." [Online]. Available: https://www.ibm.com/blockchain/industries/supply-chain. [Accessed: 31-Jul-2018].

[21] N. Kshetri, "1 Blockchain's roles in meeting key supply chain management objectives," *Int. J. Inf. Manage.*, vol. 39, no. December 2017, pp. 80–89, 2018.

[22] O. Gallay, K. Korpela, N. Tapio, and J. K. Nurminen, "A Peer-To-Peer Platform for Decentralized Logistics," *Digit. Supply Chain Manag. Logist.*, pp. 18–34, 2017.

[23] M. V. Kumar and N. C. S. N. Iyengar, "A Framework for Blockchain Technology in Rice Supply Chain Management Plantation," *Adv. Sci. Technol. Lett.*, vol. 146, no. Fgcn, pp. 125–130, 2017.

[24] Archa, B. Alangot, and K. Achuthan, "Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 218, no. 1, pp. 189–195, 2018.

[25] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and ..., "A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids," pp. 1–6, 2018.

[26] S. Aggarwal, "EnergyChain : Enabling Energy Trading for Smart Homes using Blockchains in Smart Grid Ecosystem."

[27] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and Solutions," 2016.

[28] G.-J. Ra and I.-Y. Lee, "A Study on KSI-based Authentication Management and Communication for Secure Smart Home Environments," *Ksii Trans. Internet Inf. Syst.*, vol. 12, no. 2, pp. 892–905, 2018.

[29] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. (PerCom Work.*, pp. 618–623, 2017.

[30] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri, "Autonomic Identity Framework for the Internet of Things," *Proc. - 2017 IEEE Int. Conf. Cloud Auton. Comput. ICCAC 2017*, pp. 69–79, 2017.

[31] D. Han, H. Kim, and J. Jang, "Blockchain based smart door lock system," *Int. Conf. Inf. Commun. Technol. Converg. ICT Converg. Technol. Lead. Fourth Ind. Revolution, ICTC 2017*, vol. 2017–Decem, pp. 1165–1167, 2017.

[32] A. S. Patil, B. A. Tama, Y. Park, and K. H. Rhee, "A framework for blockchain based secure smart green house farming," *Lect. Notes Electr. Eng.*, vol. 474, pp. 1162–1167, 2018.

[33] A. Chatterjee, "Artificial Intelligence based IoT Automation : Controlling devices with Google and Facebook," *Int. Res. J. Eng. Technol.*, vol. 5, no. 4, 2018.

[34] M. Singh, A. Singh, and S. Kim, "Blockchain: A game changer for securing IoT data," *2018 IEEE 4th World Forum Internet Things*, pp. 51–55, 2018.

[35] P. Ghuli, U. P. Kumar, and R. Shettar, "A Review on Blockchain Application for Decentralized Decision of Ownership of IoT Devices," *Adv. Comput. Sci. Technol.*, vol. 10, no. 8, pp. 2449–2456, 2017.

[36] C. Science, "An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology," no. March, pp. 769–773, 2018.

[37] S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh, "A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.

[38] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, "A blockchain-based trust system for the internet of things," *Proc. ACM Symp. Access Control Model. Technol. SACMAT*, vol. Part F1371, pp. 77–83, 2018.

[39] G. Varshney and H. Gupta, "A security framework for IOT devices against wireless threats," *2017 2nd Int. Conf. Telecommun. Networks*, pp. 1–6, 2017.

[40] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for iot-related deployments through blockchain," *2017 IEEE Conf. Netw. Funct. Virtualization Softw. Defin. Networks, NFV-SDN 2017*, vol. 2017–Janua, no. November, pp. 303–308, 2017.

[41] Y. Sakakibara, S. Morishima, K. Nakamura, and H. Matsutani, "A hardware-based caching system on FPGA NIC for Blockchain," *IEICE Trans. Inf. Syst.*, vol. E101D, no. 5, pp. 1350–1360, 2018.

[42] L. Zhou, L. Wang, Y. Sun, and P. Lv, "BeeKeeper : A Blockchain-based IoT System with Secure Storage and Homomorphic Computation," *IEEE Access*, vol. PP, no. 8, p. 1, 2018.

[43] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future to Internet of Things security: A position paper," *Digit. Commun. Networks*, 2017.

[44] P. Fremantle and P. Scott, "A survey of secure middleware for the Internet of Things," *PeerJ Comput. Sci.*, vol. 3, no. May, p. e114, 2017.

[45] Z. Bao, W. Shi, D. He, and K.-K. R. Chood, "IoTChain: A Three-Tier Blockchain-based IoT Security Architecture," pp. 1–24, 2018.

[46] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," *Int. Conf. Adv. Commun. Technol. ICACT*, pp. 464–467, 2017.

[47] S. Seth, "Banks Need to Be Centralized – Could Blockchain be the Answer? | Finance Magnates." [Online]. Available: https://www.financemagnates.com/cryptocurrency/bloggers/banks-need-centralized-blockchain-answer/. [Accessed: 31-Jul-2018].

[48] A. Banafa, "IoT and Blockchain Convergence : Benefits and Challenges," *IoT Blockchain Converg. Benefits Challenges - IEEE Internet Things*, no. January 2017, pp. 1–10, 2018.

[49] J. Coward, "Meet the Visionary Who Brought Blockchain to the Industrial IoT." [Online]. Available: https://www.ioti.com/security/meet-visionary-who-brought-blockchain-industrial-iot. [Accessed: 31-Jul-2018].

[50] "Blockchain Will Help Us Prove Our Identities in a Digital World." [Online]. Available: https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world. [Accessed: 31-Jul-2018]