Using Blockchain Technology For IoT Security

Majd Alhariri, Department of Information technology, College of Computer, Qassim University, Buraidah, KSA, 431114118@qu.edu.sa
Sulaiman Aldubaykhi, Department of Information technology, College of Computer, Qassim University, Buraidah, KSA, 431114111@qu.edu.sa

Submitted to
Dr.Murad Qasem, Department of Information technology, College of Computer, Qassim University, Buraidah, KSA, m.qasem@qu.edu.sa

Abstract:
The IoT technology spread widely into the world but still has challenges to address, especially in the security part. We talk about the history of the blockchain, and how it is important to provide a high level of security for IoT and the advantage that could be obtained if the integration happens, and many of IoT challenges can be addressed with this integration.

Keywords: Blockchain technology, Internet of Things technology, Blockchain and IoT integration, IoT Security, Network security, Data security.

1.Introduction

In our time, smart devices and the speed of data transmission over the network have become very fast. In recent times, the Internet of things (IoT) has gained great acceptance and popularity among people. The IoT is a huge ecosystem that includes a wide range of areas, such as home use, for example, smart refrigerators and smart door locks, and also in the agricultural and health aspect, etc [1,2]. The IoT is replacing the human workforce, as it takes place between human and machine interaction where there is an interaction between human and machine [3].

Figure **1** shows the high-level architecture of the IoT, which consists of the application layer, the processing layer, the network layer, and the perception layer. The application layer is to meet the needs of the end-user and includes smart homes, healthcare, smart robots, etc. The processor layer is responsible for databases and servers and performs many operations such as making decisions and storing a lot of data. The network layer contains many types of

communication networks, for example, Wi-Fi, Bluetooth, LoRa, etc. And is responsible for transmitting information to the next layer. The last layer is the perception layer, which is responsible for the sensor devices, security cameras, robots, etc. Where these devices collect sensory data for storage.

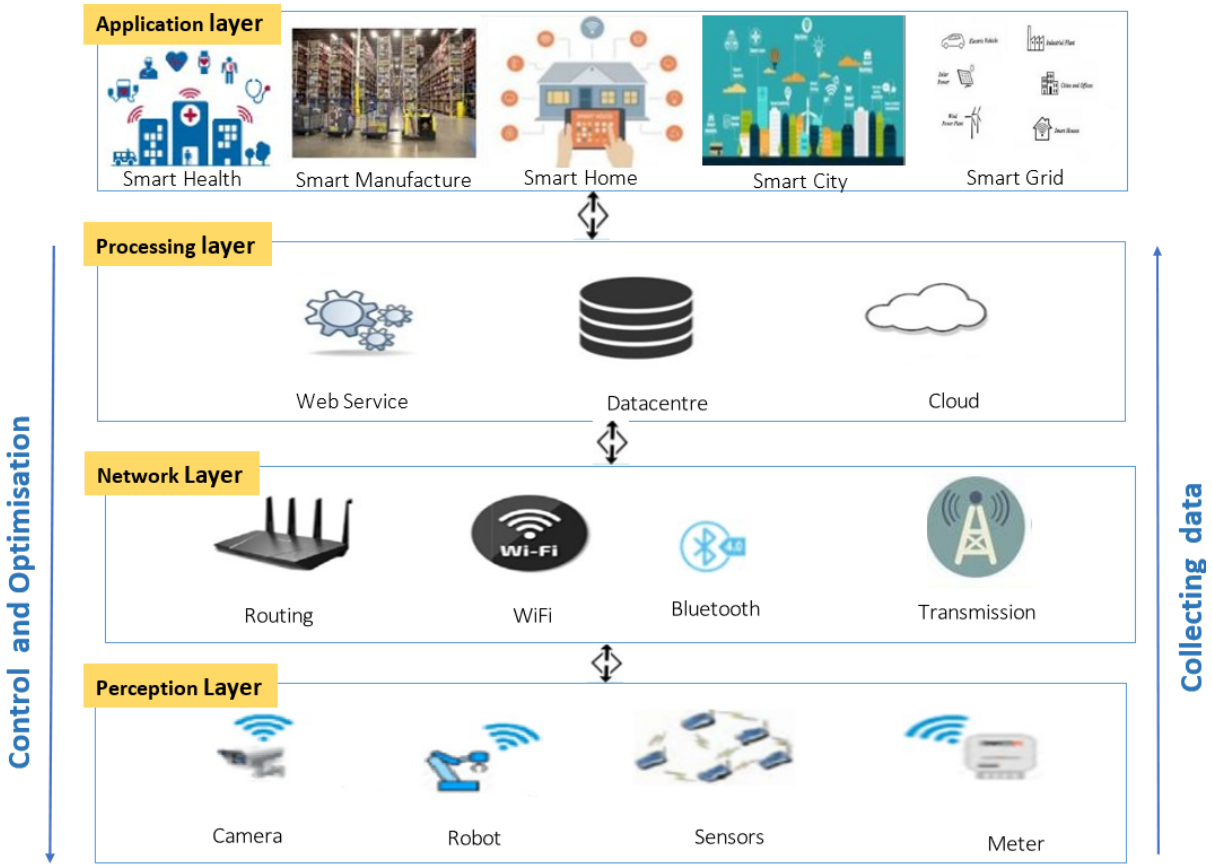

figure 1: high-level architecture of the IoT

In 2017, a lot of security vulnerabilities appeared in IoT devices, as the number of attacks increased to 280%, and in 2021, companies spent on information security protecting IoT devices from $83.5 billion to $119.9 billion as they depend on the infrastructure of the Internet of Things.

Many protocols were used to eliminate security risks, but they were not enough.
Blockchain technology could be so important to secure the internet of things (IoT).
There are about a billion devices connected and communicating to each other and increasing every year[9]. The information that flows via IoT must remain secure. In **figure** 2, these are some examples of attacks on the IoT with different layers [9].

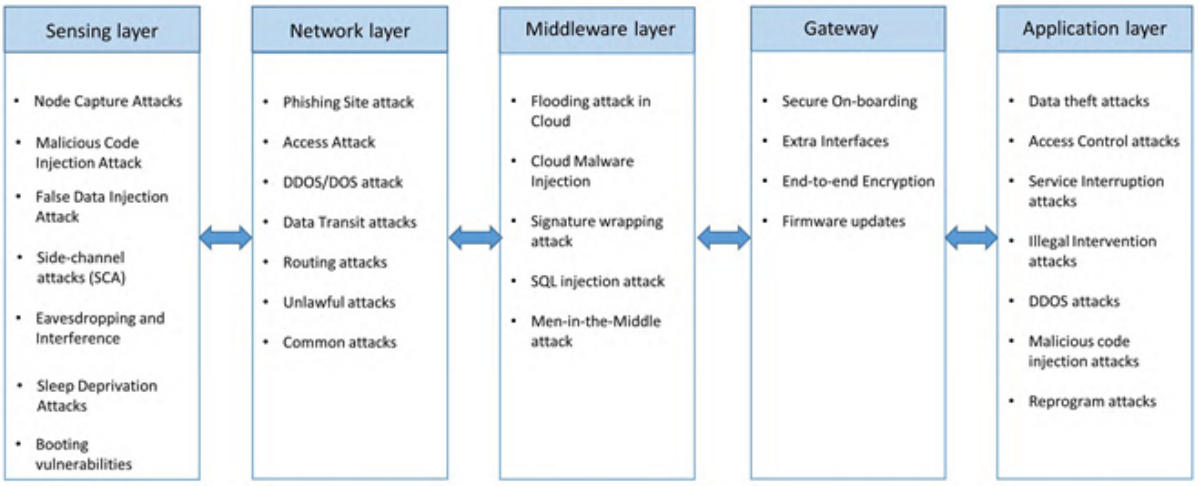

Figure 2: Types of attacks on IoT.

The Blockchain is a Peer-to-Peer network (P2P) that records history with distributed ledger technology, relies on shared database and encryption algorithms technology to connect between several devices on the internet . Blockchain Technology (BT) can solve trusting-relevant issues. using Hash Chain Based Encryption (HCBE) in secure transmission and time stamp mechanism of certificate value for modification and data traceability ensures. The Blockchain Technology revolution will change many aspects of the Internet of Things systems (IoTs). Figure 3 shows some characteristics of blockchain technology [34].

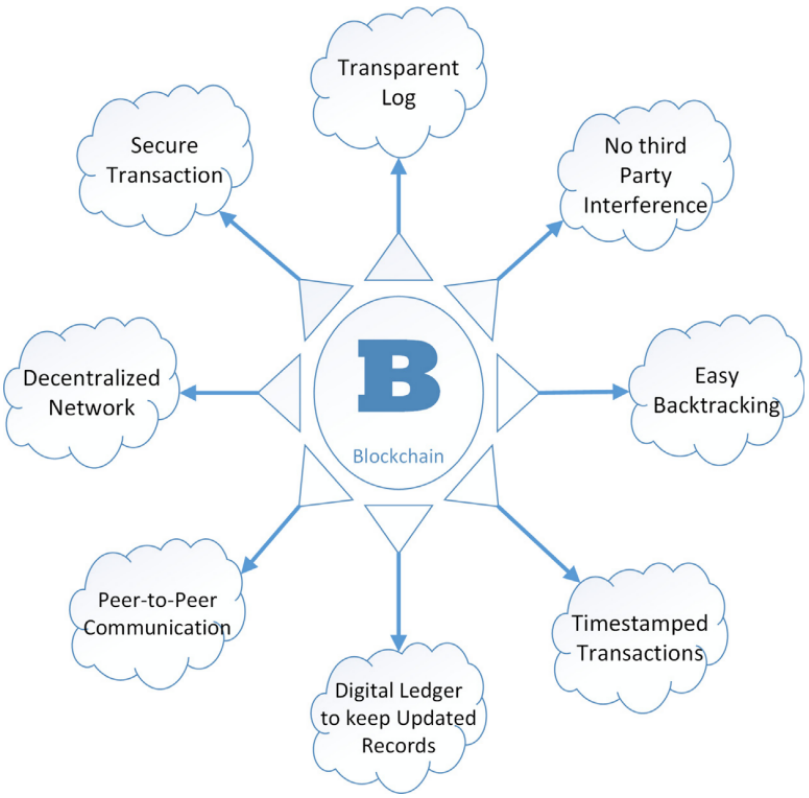

figure 3: characteristics of blockchain technology

Blockchain Technology has a strong security system that relies on communication Technology, consensus mechanism and the cryptography algorithms [2].
This article will solve security and privacy problems and trust issues through the use of Blockchain Technology (BT) and review some articles regarding IoT security using blockchain technology and how to secure the connection between IoT devices and users without third party interference.

1. Blockchain technology ensures the security of the IoT by placing trust mechanisms between devices within the IoT system as it provides a mechanism that does not require trust between nodes.

2. Blockchain also will reduce the cost of equipment and increase the performance of IoT systems. The blockchain provides a full use of storage capacity and computing and broadband of distributed idle devices of IoT and reduces storage costs and calculations.

3. Blockchain increases the reliability of the IoT, and ensures that even if one or more nodes are attacked, the data of the entire network is secure.

2.Blockchain history and Applications

2.1. History of blockchain technology:

Blockchain technology uses different types of other technology such as Markel trees and cryptographically secure-chain of blocks [4,5] when developed in the early 1990s. The first use of Blockchain was in Conceptualized and Implemented Satoshi Nakamoto 2008[6]. The first implementation of this technology was bitcoins as we can see in **figure** 4.

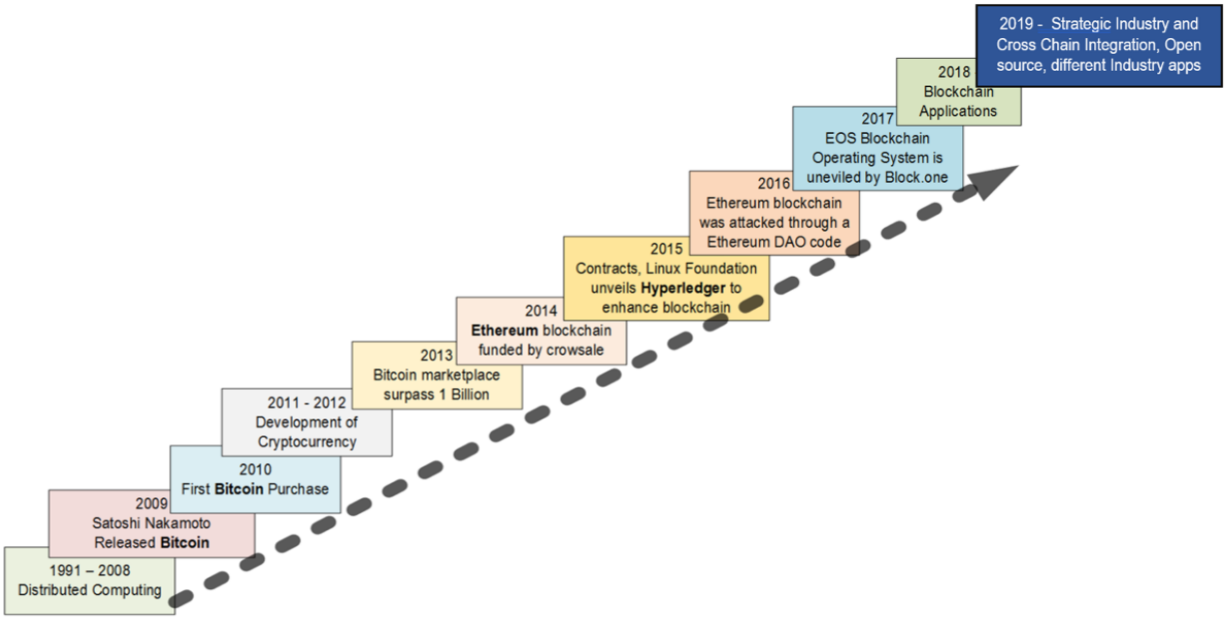

Figure 4. History of Blockchain technology.

2.2. Applications and use cases of Blockchain:

There are different applications and use cases using blockchain technology as **figure** 5 shows, it shows a simple overview in the following section of each domain.

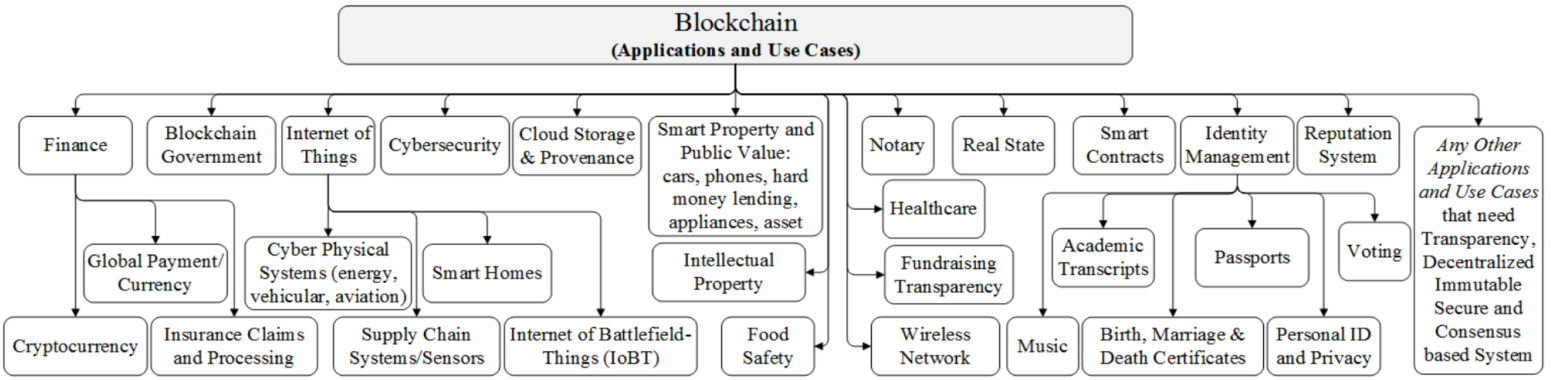

Figure 5. different Applications and Use cases of Blockchain technology.

3.Related surveys

In this article, we will provide an overview of previous articles that dealt with the uses of blockchain in IoT security, and we will also provide a detailed overview of blockchain technology and the IoT. **Table 1**, shows previous research that used blockchain technology in IoT security.

In [12], they worked on solutions to modern security trends in the IoT, in the field of networks and encryption methods in the IoT, and the Blockchain was addressed to help in forming the security of IoT networks, on the other hand, In this survey [7], an analysis of the IoT security framework was conducted for the development of industrial IoT applications, also, the security measures for each framework were highlighted to achieve immunity against attacks on the IoT, but the blockchain technology was not used in it.

In [11] discuss issues about IoT security in terms of, the overall architecture of IoT and security issues for different types of IoT devices. Also, thorough research was conducted on security problems in the IoT system. After that, a review of different technologies and credibility of IoT data, in addition to the use of ML and DL algorithms, and also a proposal for blockchain technology for use in protecting IoT data.

In this survey [8], the issues and challenges related to secure connection, communication and information exchange on the IoT were clarified, but blockchain technology was not mentioned on the other hand, in [9] the authors proposed the use of blockchain technology to

reduce security threats in the IoT, as well as a detailed review of other current and future threats related to IoT security, in addition to discussing the latest IoT security technologies.

In this work [10], the author discussed the development of security for IoT programs, but the blockchain technology was not mentioned at all. They suggested other solutions in addition to classifying some attacks on IoT security and suggesting solutions for them, also in [13] the authors did not discuss ways to protect IoT security using blockchain technology, they only discussed the components of IoT systems, their weaknesses and security implications, as well as raising the level of awareness in IoT security.

In Survey [15], the author discussed some of the current problems of the Internet of Things in cities and military uses to find solutions to these problems, in addition to the use of blockchain technicians in the security of the Internet of Things, and in the last survey [14], blockchain technology was mentioned in a simple way, focusing on open issues and future research gaps in IoT security, in addition to in-depth reading of research references in the field of IoT security.

Table 1. Comparison of previous survey articles about using (BT) in IoT security.

Survey articles	Year	Description	Using (BT) in IoT security	Ref
Security trends in IoT	2021	Solutions about recent security trends in the IoT in the field of networks to develop protocols and encryption methods in the IoT.	✓	[12]
Security of IoT frameworks	2018	Conducting an analysis of the security framework of the IoT and clarifying the basics and architecture of smart applications	×	[7]
IoT Security Issues, Vulnerability and Challenges	2020	Searching for solutions to problems related to the security of the IoT. Suggesting technologies for the security of the IoT information, as well as solutions for the security of the IoT environment.	✓	[11]

Security in IoT Environment	2016	Securing connection, communication and exchange of information in the security of the IoT	×	[8]
IoT Security Security Threats and solution	2019	A detailed review of the challenges and security sources related to the IoT and providing solutions to current and future security threats	✓	[9]
Security Attacks in IoT	2017	Discuss and classify attacks in the IoT. Develop IoT programs from the security side to avoid attacks on IoT devices.	×	[10]
Enterprise IoT Systems	2021	Discussing components of Enterprise-IoT systems as well as vulnerabilities and their security implications, to raise awareness about Enterprise-IoT systems and stimulate further research.	×	[13]
IoT cybersecurity and risk	2021	Discuss some of the current problems of the IoT in cities and military uses with a number of scientific research in order to find solutions to these problems and set some points for future research	✓	[15]
Manufacturers in the security of the IoT	2021	Discuss open issues and future research gaps in the security of the IoT, and give future research a clear path for research	✓	[14]

4. Blockchain and IoT integration (challenges and opportunities) :

Although the main idea of Blockchain is soft, implementation faces a different type of challenges. The internet of things (IoT) converts and improves manual-operations to digital information, obtaining sets of data that provide unheard levels of knowledge. this knowledge can help in optimizing the development of smart applications such as the quality of lives and improve the management in the cities through digitizing services in cities, in a few years ago, cloud computing technology helps to improve the IoT using functionality to process and analyze the information and transformed into a real time action [16]. This progress in IoT changes so many challenges into new opportunities in our community such as accessing and sharing information. but every technology has vulnerabilities and the biggest vulnerability that has occurred in different situations is trust. Centralized architectures such as the one that is used in cloud computing have contributed to the development of IoT. However, data transparency works as a black boxes and the others do not have a clear knowledge of how and where the information they gives, is going to be used. The problems of trust in systems are acutely complex when no auditing or verification techniques are used, especially when they are dealing with sensitive information like economic transactions with virtual currencies.

Blockchain also can boost IoT with a trusted sharing service where information is traceable and reliable. Data remains immutable and data sources will be identified at any time , this will significantly increase the security. If any data leak in any partition in the chain fraudulence or slowing down the process of detecting and addressing the problem, this can significantly affect lives, countries and sectors in the case of the foodborne outbreak and lead to huge economic and financial losses [17].

Blockchain technology is the solution for reliability, scalability, and privacy problems that is related to IoT technology as we can see in [18]. As we can see there are so many advantages to use from Blockchain technology in IoT technology, these two technologies can provide greatly benefit to our communities with each of them and more if mariging them together, there is a huge number of studies and research challenges that can be studied and developed in this topic.
this is some improvement can come from this integration:

- **scalability and decentralization:**
  The shifting from centralized architecture P2P will remove the central point of bottlenecks and failures[19], also it will help in preventing some cases such as

if a few huge companies manage control and processing of a large number of people, improve the fault toleration and scalability, improving the IoT scalability and reduce the IoT silos.

- **identity:**
  If using a common blockchain system, participants are able to identify the other participants' devices and the data that is provided to the system is immutable and accurately recognizes the actual data that is provided by each device. However, blockchain technology can provide trusted authentication and authorization distribution of IoT devices [20].

- **Reliability:**
  IoT data can remain distributed and immutable over time in blockchain [21]. Participants in this system can verify and identify every single device and the authenticity of the provided data and they will be sure that the data integrity is trusted. Reliability is the main point of using blockchain technology in IoT.

- **Security:**
  Blockchain can secure the communication between devices by treating the message exchange as a transaction checked by smart contract. communication and information will be widely secure if stored as a transaction of the blockchain[22]. IoT technology uses a secure standard- protocols, it can be improved with the blockchain applications [23].

- **Autonomy:**
  Using blockchain technology devices can act by themselves without any server involved in the operation. IoT applications can get many advantages from this functionality such as decoupled applications and agnostic devices. The blockchain technology will support the applications of the next generation and provide development of the smart autonomous assets and hardware as a service like in [24,25].

- **secure coding deployment:**
  by using the secure-immutable storage of the blockchain, inputting code into the devices can be safe and secure [26,27]. Manufacturers can be able to track

updates and states of each device with a high level of confidence[26]. IoT middlewares can securely update IoT devices by using this functionality.

- **Market and Purchase Services (MPS):**
  The blockchain improved the acceleration of making data marketplace and IoT ecosystem service, and made transactions between two users possible without needing third party services. microservices could be easy and safe even if it's made in a trustless placement, micropayment as well, some ways in [29,30,31].

When integrating the blockchain it has to be decided in which part between the underlying IoT infrastructure, there are three techniques or alternatives that the communication can use: inside the IoT, a hybrid design involving blockchain and IoT, or via blockchain. Also Fog computing added a new layer between IoT devices and cloud computing and the blockchain that could make this integration more simple.

Figure 6 will show these alternatives and described advantages and disadvantages of each one :

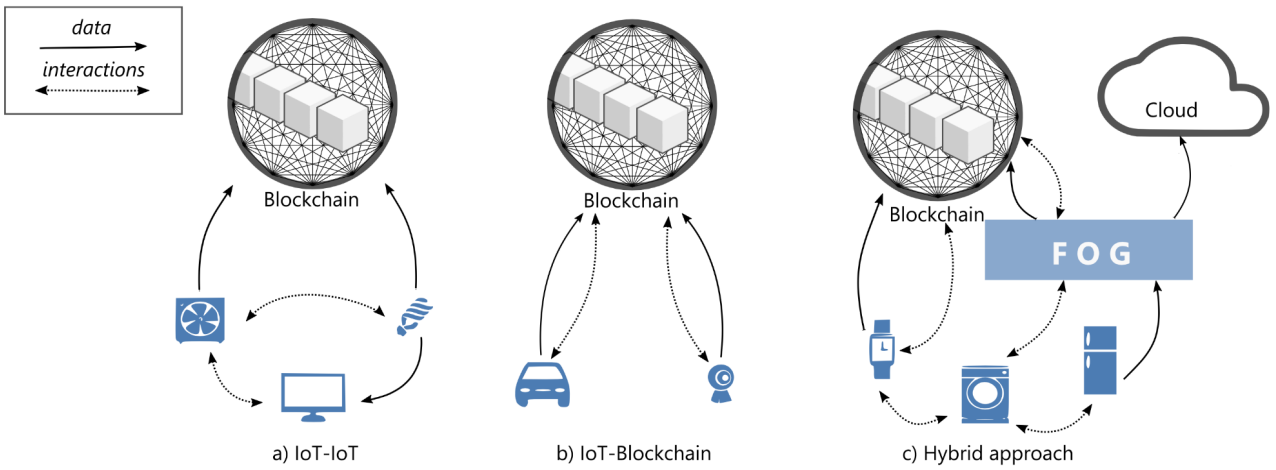

Figure 6: IoT and Blockchain Interactions approach

A. IoT-IoT approach:

In this approach, IoT devices can communicate with each other, with routing and discovery mechanisms. This type of interaction is the fastest in terms of latency and security and is able to work offline. Blockchain will only store only a part of IoT data where the IoT interactions happen without blockchain involved in the process (figure 6.a). This interaction can be useful in some scenarios with reliable data of IoT where the interactions work with low latency.

B. IoT-Blockchain approach:

In this type of approach, every interaction goes via blockchain, allowing an immutable record list of interactions. increase the autonomy of IoT devices and trace all the chosen interactions and their details will be queried in the blockchain (Figure 6.b). IoT applications that use to trade or rent can take advantage of this approach to provide their services. storing all the interaction in the blockchain could increase in data and bandwidth, this is one of the common challenges in blockchain. all the IoT data that is involved in this transaction have to be stored in blockchain

C. Hybrid approach:

This is the last approach, where only a part of the interaction and data takes a part on the blockchain, the rest of the data and interaction are directly shared between the IoT devices. The challenge in this approach is which interaction has to go via blockchain and finding a way to choose it in run time. The perfect Coordination of this approach can be the best way to integrate between blockchain technology and IoT technology and take advantage of blockchain features and the advantage of the IoT real-time interaction. In this approach fog computing and also cloud computing will complement the limit of the blockchain and IoT. Fog computing uses a fewer computationally-limited devices like gateways , where mining can be used in the same way as other initiatives that used the IoT devices such as [32,33].

5.Conclusion

These two technologies will provide a lot of things to the current technologies that are used in our world, the Internet of Things and the Blockchain make a great revolution in many things in the world such as healthcare and economics. If we integrate these two technologies together it will provide a large number of benefits with a high level of security that we can use in our community. In this survey, the IoT was discussed in general, and in particular the security of the IoT, as well as the use of blockchain technology in protecting the security of the Internet, and the previous surveys were discussed to compare it in this survey to consider whether they use the blockchain technology in the security of IoT or not.

references

1. Khan, Minhaj Ahmad, and Khaled Salah. "Iot Security: Review, Blockchain Solutions, And Open Challenges". *Future Generation Computer Systems*, vol 82, 2018, pp. 395-411. *Elsevier BV*, doi:10.1016/j.future.2017.11.022.

2. "Embedding Blockchain Technology Into Iot For Security: A Survey". *Ieeexplore.Ieee.Org*, 2021, https://ieeexplore.ieee.org/abstract/document/9358215. Accessed 2021

3. Kumar, Nallapaneni Manoj, and Pradeep Kumar Mallick. "Blockchain Technology For Security Issues And Challenges In Iot". *Procedia Computer Science*, vol 132, 2018, pp. 1815-1823. *Elsevier BV*, doi:10.1016/j.procs.2018.05.140.

4. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. In *Conference on the Theory and Applications of Cryptography*; Springer: Berlin/Heidelberg, Germany, 1990.

5. Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*; Princeton University Press: Princeton, NJ, USA, 2016.

6. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/ bitcoin.pdf (accessed on 10 September 2020)

7. Ammar, Mahmoud et al. "Internet Of Things: A Survey On The Security Of Iot Frameworks". *Journal Of Information Security And Applications*, vol 38, 2018, pp. 8-27. *Elsevier BV*, doi:10.1016/j.jisa.2017.11.002.

8. R. Joshitta , L. Arockiam “Security in IoT Environment: A Survey”. R. Shantha Mary Joshitta et al, Int. Journal of Information Technology & Mechanical Engineering - IJITME, Vol.2 Issue. 7, July- 2016, pg. 1-8.

9. Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. 27 February 2019. Document ID:1551296909190103. Available online: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html (accessed on 10 September 2020).

10. J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 32-37, doi: 10.1109/I-SMAC.2017.8058363.

11. Patnaik, Ranjit et al. "A Systematic Survey On Iot Security Issues, Vulnerability And Open Challenges". *Advances In Intelligent Systems And Computing*, 2020, pp. 723-730. *Springer Singapore*, doi:10.1007/978-981-15-5400-1_68.

12. Rachit et al. "Security Trends In Internet Of Things: A Survey". *SN Applied Sciences*, vol 3, no. 1, 2021. *Springer Science And Business Media LLC*, doi:10.1007/s42452-021-04156-9.

13. Rondon, Luis Puche et al. "Survey On Enterprise Internet-Of-Things Systems (E-Iot): A Security Perspective". *Arxiv.Org*, 2021, https://arxiv.org/abs/2102.10695. Accessed 14 Nov 2021.

14. N. Mazhar, R. Salleh, M. Zeeshan and M. M. Hameed, "Role of Device Identification and Manufacturer Usage Description in IoT Security: A Survey," in IEEE Access, vol. 9, pp. 41757-41786, 2021, doi: 10.1109/ACCESS.2021.3065123.

15. Choo, K., Gai, K., Chiaraviglio, L., & Yang, Q. (2021). A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. *Computers & Security*, *102*, 102136. doi: 10.1016/j.cose.2020.102136

16. M. D´ıaz, C. Mart´ın, B. Rubio, State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing, Journal of Network and Computer Applications 67 (2016) 99–117.

17. J. C. Buzby, T. Roberts, The economics of enteric infections: human foodborne disease costs, Gastroenterology 136 (2009) 1851–1862.

18. H. Malviya, How blockchain will defend iot, Available online: https://ssrn.com/abstract=2883711, 2016. Accessed: 2018- 02-01.

19. P. Veena, S. Panikkar, S. Nair, P. Brody, Empowering the edge-practical insights on a decentralized internet of things, Empowering the Edge-Practical Insights on a Decentralized Internet of Things. IBM Institute for Business Value 17 (2015).

20. S. Gan, An IoT simulator in NS3 and a key-based authen- tication architecture for IoT devices using blockchain, Ph.D. thesis, Indian Institute of Technology Kanpur, 2017.

21. modum, Available online: https://modum.io/, 2017. Accessed: 2018-02-01.

22. G. Prisco, Slock. it to introduce smart locks linked to smart ethereum contracts, decentralize the sharing economy, Available online: https://bitcoinmagazine.com/articles/ slock- it- to- introduce- smart- locks- linked- to- smart- ethereum - contracts - decentralize - the - sharing - economy - 1446746719/, 2016. Accessed: 2018-02-01.
23. M. A. Khan, K. Salah, Iot security: Review, blockchain so- lutions, and open challenges, Future Generation Computer Systems (2017).

24. Blockchain of Things, Inc. (BCoT). (2021). Retrieved 17 November 2021, from https://blockchainofthings.com/.

25. Filament.com - Buckley Media: Exclusive Brokers for Filament.com. (2021). Retrieved 17 November 2021, from https://www.buckleymedia.com/filament.html.
26. P. Veena, S. Panikkar, S. Nair, P. Brody, Empowering the edge-practical insights on a decentralized internet of things, Empowering the Edge-Practical Insights on a Decentralized Internet of Things. IBM Institute for Business Value 17 (2015).

27. M. Samaniego, R. Deters, Hosting virtual iot resources on edge-hosts with blockchain, in: Computer and Information Technology (CIT), 2016 IEEE International Conference on, Yanuca Island, Fiji, IEEE, 2016, pp. 116–119.

28. G. Prisco, Slock. it to introduce smart locks linked to smart ethereum contracts, decentralize the sharing economy, Available online: https://bitcoinmagazine.com/articles/ slock- it- to- introduce- smart- locks- linked- to- smart- ethereum - contracts - decentralize - the - sharing - economy - 1446746719/, 2016. Accessed: 2018-02-01.

29. MyBit. (2021). Retrieved 17 November 2021, from https://mybit.io .

30. Crunchbase Pro. (2021). Retrieved 17 November 2021, from https://about.crunchbase.com/products/crunchbase-pro/

31. The Future of Energy | Pando | LO3 Energy. (2021). Retrieved 17 November 2021, from https://lo3energy.com/ .
32. Eth(Embedded) – Ethereum Clients on Embedded Devices. (2021). Retrieved 19 November 2021, from http://ethembedded.com/ .
33. raspnode. (2021). Retrieved 19 November 2021, from https://raspnode.com/.

34. Hassan, Muneeb Ul et al. "Privacy Preservation In Blockchain Based Iot Systems: Integration Issues, Prospects, Challenges, And Future Research Directions". *Future Generation Computer Systems*, vol 97, 2019, pp. 512-529. *Elsevier BV*, doi:10.1016/j.future.2019.02.060.