Use of Blockchain to Support the Security of Internet of Things: A Review

[1]Saher Un Nisa , [2]Maryam Khalid
[1] Department of Computer Science, University of Lahore, Gujranwala, Punjab, Pakistan
Saherrajput372@gmail.com
[2] Department of Information Technology, University of Lahore, Gujranwala, Punjab, Pakistan
Maryamkhalid272@gmail.com

Abstract
Internet of Things (IoT) is now spreading everywhere. It's the technology of every person's need so we can't step back from IoT but we can secure it as it is spreading quickly so it has greater chances of danger and being misused. There is an urgent need to make IoT devices secure from getting cracked or hacked. A lot of methods had tried and still trying to mitigate IoT security issues. In this paper Blockchain is going to be the solution of most of the IoT issues or problems.We have discussed or highlighted security issues with centralized IoT and then provided solution of such security challenges through the use of blockchain because is based on a decentralized technology that is hard to modify or update.

Keywords:
IoT (Internet of things), security, Privacy, Blockchain , Centralize d , Decentralized .

1. Introduction

The internet is very important in our daily life. By using set of communication protocols we can connect with the world. In the beginning, internet had limited means of communication like email services but now internet is everywhere and by using new apps we can connect to any corner of the world. Currently intelligent devices are mandatory and essential chunk of our lives in which it unites different belongings or things remotely at every time. The number of linked smart devices is growing everyday therefore it is the time of necessity to secure the IoT devices as users are using IoT devices uninterruptedly for every purpose so it is a time of need when we have to secure our IoT devices for keeping our Private data secured. The term IoT means internet of things that connects various things or devices to the Internet So physical components can communicate by using intelligent terminal without the need of any human interaction [10].IoT is expanding every single day. It is giving access to humans and all the objects and devices in their surroundings to get connected all over the internet for sharing their particular data, resources and creating new applications and web services which gives consequences in a more appropriate connected world. IoT is using centralized architecture that has so many problems because everything is carried out in a network using a single server. It can be concluded that this centralized system creates a lot of tension or problem as single point of failure will make the server goes down and the complete system will become unreachable [2]. IoT central design can be easily targeted for security and privacy. Because everything that is carried out on a single link that is underneath the power of a single server can be easily hacked .In addition, central architecture also has scalability concerns as it is worthy for businesses or dealings at small level but for huge businesses it would be unfeasible that have numerous offices all around this world.

Researchers are focusing on the solving the issues relate to IoT from past few years, they are trying to address the issues regarding security, scalability and communication [22],[23],[24]. On another side, DLT ("Distributed Ledger Technology") got lot of success in securing IoT devices. DLT runs an undeniable ledger that cannot be transformed by anybody and escaped the need for a central or national reliable third party which would be responsible for particular transaction [11].

There are more than a few barriers in IoT central structure, Communication between the IoT devices by a DLT maybe the best choice. DLT is a well-known variety of the the BC. It can be described as a ledger that is dispersed and based on decentralized communications and trades to manage a nonstop developing institution of data. For a deal or transaction within the ledger, the mainstream nodes taking part inside the blockchain network that majority must have to agree and file their agreement. Hard and fast transactions bring together and assign a block within the ledger that is a chain of blocks. For making a connection between blocks collectively every block includes hashing feature and a timestamp of the preceding block. The hash feature validates reliability and non-refusal of statistics inside the block. Furthermore, all the nodes that are participating in the network hold a unique duplicate of ledger so that after every change they will be synchronized.

Manuscript received July 5, 2023
Manuscript revised July 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.7.17

For instance, implementing the distributed architecture for IoT appliances can help in clearing up countless dilemmas in actual safety and socket failure. As blockchain deals with decentralized environment where no administration is required for the accomplishment, implementation of activities and communication control between several nodes inside this network. This in turn is governed by the environment where participating nodes are only substances to receive or reject a transaction based on the agreement [8]. Remaining paper is set in a way that Section 2 contains related work. Section 3 will define some IoT boundaries or limitations .In section 4 a brief introduction of BC is presented .Section 5 is showing combination of IoT with BC technology. Finally section 6 contains conclusion of the work.

2. Related Work

Information collected from URL: "https://www.postscapes.com/iot-history".
The idea of internet of thing was given by kavin Ashton and IoT has started it"s life in a presentation at "Procter and gamble" in 1999.[1]He linked the novel hint of RFID in PG source chain [6].
1999: IoT principles told by Neil Gershenfeld for the first time in his book whose title is "When Things Start to Think"
(2003-2004): "RFID is deployed on a massive scale by the US Department of Defense in their Savi program and Wal-Mart in the commercial world."
(2008-2009): "The IoT was born according to Cisco"s Business Solutions Group. Blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin" [7].
2010: "Chinese Premier Wen Jiabao calls the IoT a key industry for China and has plans to make major investments in Internet of Things".
According to Gartner [9], it is predictable that "The number of Internet-linked devices will increase from around 25 billion to 50 billion by 2020" [5].

3. Boundaries of Centralized Model of IoT

Although Internet of things breeds a lot of novelties and have a beneficial effect on current environment as compared to the traditional environment but still it has a lot of limitations that could be dangerous if not solved [3].There are several obstacles related to the IoT centralized architecture. In this session some of them will be highlighted.

- **Scalability:**

It is a most important matter to solve as IoT is based on a central authority Who is controlling and managing each and every process of the system. However this system can be scaled properly but only for small networks for bigger networks it has limitations so to deploy a centralized system at high scale would really be an impractical decision .As we all are familiar that the use IoT devices are increasing every day so centralized architecture would be unable to meet the demands of increasing devices in coming future [15].

- **Cost of the network:**

All nodes in the network assisted by software and hardware should have the ability to provide sufficient support as all operations of computer are implanted by the central server. Multiple nodes involved in communication and have a huge amount of data for transfer so server needs extraordinary processing power to help various nodes simultaneously. It involves huge data storage of multiple devices that requires a cost of storage capacity and maintenance. Overall, IoT requires extremely expensive maintenance for the placement, preservation of centralized server with the growing IoT devices [18].

- **Confidentiality:**

The Central system is weak or vulnerable in data transactions. Data can contain sensitive information of nodes like someone's account details, password or it could be a financial transaction so this centralized network collect all data at a single point or at a single place so the confidentiality will get effected and data is at a single place due to that it can be breached .Also service facilitators can steal private information and can pass to other companies for their personal benefit so it has concluded that IoT is lacking in providing confidentiality [19].

- **Safety:**

Security is a main issue in IoT devices .The centralized server is responsible for all transactions and data storage as everything is stored at a single point or place so data can be easily hacked also the users does not know about the data that is transferred tat where the data is going and how tis data will be used. It is a complete black box where users can't see what's going on. Also increasing numbers of IoT devices and their need making security very low that is really dangerous as companies are trying to innovate new gadgets but security is not at prior level in their lists [14], [17].

- **Solo Plug Disaster:**

The centralized server is responsible for transaction and all the participating nodes are attached to it so single

point of failure will make the entire system out of access so redundant switches, a lot of different
Network links and backup servers arranged in order to avoid these kind of problems but it takes a lot of power and expenditures .in case of server connection failure sometimes synchronization between original server and backup create problem .

- **Access and Variety**

The participating nodes can access the network for different needs however centralized system bound them to use or follow identical procedures for getting details from network so it is affecting the flexibility of the network because it is limiting the variety in the network and stopping some of the participated nodes from gaining access to network [13].

- **Inflexibility:**

All transactions and processing of the network is dependent on to the centralized network as so many nodes are connected to the network that will bring a massive workload on centralized server. During peak hour's system become inaccessible as majority wants to access the central system at the same time that made the network so busy and flexibility of the network get effected while users trying to complete their work[17].

4. What is Blockchain Itself and how does it work.

A Blockchain is a diary that is practically impossible to forge. It is a digital ledger that keeps a record of endlessly growing set of data. In this decentralized system, there is no main computer who is managing the whole chain. As an alternative, all contributing nodes have a copy of the chain. A blockchain comprises of two kinds of elements:

- Transactions are formed by the members of the system.
- Blocks record these dealings in the precise order and do not allow any interference. Blocks record a time stamp too when the transactions were added.

So when somebody wishes to add a transaction into the chain, all the members in the network will authenticate or validate it. They do this with the help of an algorithm to the transaction to prove its validity. Then a majority of the members have to agree that the transaction is valid. A list of permitted communications or dealings is then pushed in the block, which will send to total number of nodes in the network. They in turn authenticate the new block. Each consecutive block holds a hash, which is a matchless fingerprint, of the preceding block.

5. Blockcain Integration with IoT

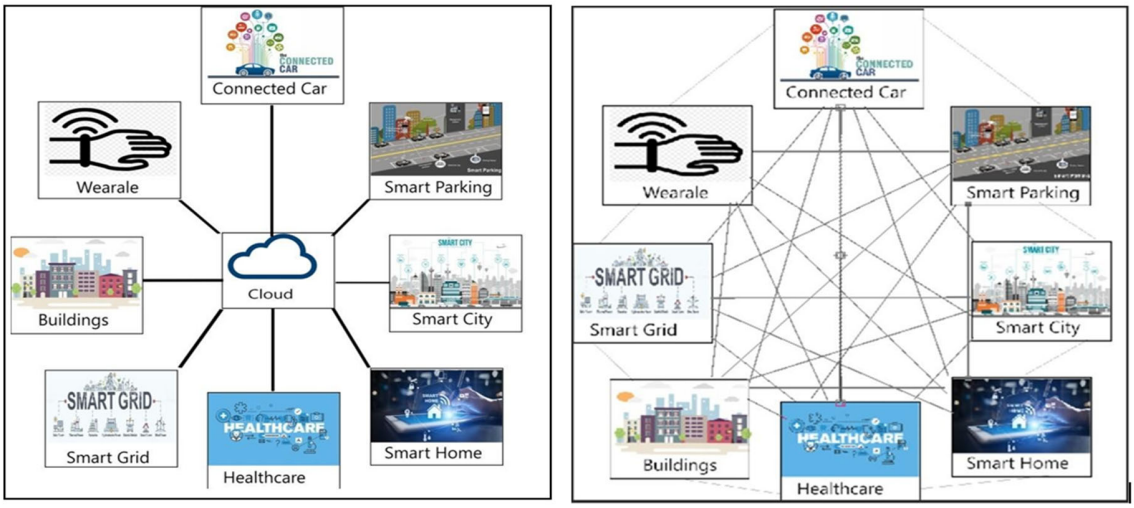
The unexpected growth of IoT has revealed new openings in different fields [17]. Nevertheless, the main hurdle for the guaranteed delivery of IoT devices is the absence of belief, trust and guarantee. As the current IoT depends on Central architecture that requires a third party supplier for managing and controlling all data composed or gathered from IoT devices without knowing how this collected data would be used. Cloud computing is contributing in the expansion IoT that is based on a Centralized architecture. The server of the centralized architecture works as a black box where the members of that particular network are not able to see that how and where the collected data is being used. The encouraging technologies like cloud computing and IoT has great value. Similarly, in the revolution of IoT the huge potential of BC has admitted. IoT security can be enhanced by BC by providing a trust worthy network where the delivered information is traceable .The use of BC will balance the IoT with reliability and security of information. For solving scalability, privacy, and reliability glitches associated with IoT paradigm BC technology is considered to be the best key factor as stated in [21]. Transaction through BC requires the contribution of all the nodes inside the network in this way data transparency is at peak. As BC use the decentralized network so there is no risk of network failure if any node gets down. Let's have a look on to the comparison table for clear understanding and need of integration. There are many resemblances and dissimilarities between IoT and BC.

Table 1: Present the most interesting facts of both technologies.

Items	Blockchain (BC)	Internet of things (IoT)
Resources or Assets	Consume resources	Restricted

Confidentiality	Ensure confidentiality	Lacking in confidentiality
Scalability	Poor scalability for big network	It contains a great variety of gadgets
Security	More Secured	Less Secured
Structure of System	Decentralized	Centralized
Trust	Provide end to end trust	Deficiency of trust
Flexibility	It provides flexibility	Flexibility demands massive expenditures

Table 1: Contrast Of IoT and BC



Centralized IoT **Decentralized IoT**

Fig. 1 Presentation Centralized IoT where a central power is responsible for communication and a Decentralized IoT Where no central authority is managing anything but a lot of members making it secure.

Table 2: The demanding situations of IoT addressed by Blockchain

IoT Challenges	How blockchain mitigate IoT issues
Flexibility	With numerous marketable and fully open source choices for BC, that is promising for IoT administrations to practice it to realize a number of goals without investing charges on investigation and improvement.
Verification and access controller	The BC keen contracts have ability to provide decentralized verification procedures and reason that can allow operational verification for devices connected by IoT.
Data Integrity	BC is a highly trusted network and provides a tempered proof ledger which is unable to update unless participating nodes pass that consent and verify that update.

Ownership and identity	BC is a trustworthy network and it offers an authorized identity registration. It's highly effective in monitoring products or items at high scale [16].
Security	A lot of nodes participating in the current network of blockchain enhance the integrity and security of the network as every change has a time stamp and signature and for transaction a lots of interconnected nodes take responsibility [12].
Other party Authority	As BC is decentralized and provide distributed network to IoT Devices so there is no need of third party for building trust between Communicating nodes.
Point of failure	BC is decentralized network and when there is no centralized Network then there is no fear of point of failure of the network.

As a result, Blockchain offer such features or situations that are not possible without it. Table 2 shows the issues of IoT and how they addressed by Blockchain.

6. Conclusion

This paper dealt with privacy and security problems of IoT . Though IoT devices gives a lot of comfort but not secured so we highlighted one of the technology which is Blockchain Integrated with IoT for creating more secure , trustworthy ,authenticate and error prone network .Security issues related to IoT have discussed and desirable solution is given by using blockchain .Centralization Vs. Decentralization concept is presented. Hope this paper would give basic idea to understanding the need of blockchain in IoT .Blockchain has ability to Provide Trusted transaction, coordination enhance transparency and auditing. Blockchain products are being developed. Compliance with the information privacy regulatory framework desires to be taken into consideration, as it is able to affect essential components of an envisaged solution because blockchain ,IoT integrated systems are vulnerable too several privacy fears that needs to be determined before their technical implementation so In future developers must take it into consideration for the betterment of the new integrated system and for enhancing trust of people.

References

[1] Kevin Ashton et al. That 'internet of things' thing. RFID journal, 22(7):97–114, 2009

[2] Hany F Atlam, Ahmed Alenezi, Madini O Alassafi, and Gary Wills. Blockchain with internet of things: Benefits, challenges, and future di- rections. International Journal of Intelligent Systems and Applications, 10(6):40–48, 2018.

[3] Hany F Atlam, Robert J Walters, and Gary B Wills. Intelligence of things: opportunities & challenges. In 2018 3rd Cloudification of the Internet of Things (CIoT), pages 1–6. IEEE, 2018.

[4] Nicola Fabiano. Internet of things and blockchain: legal issues and pri- vacy. the challenge for a privacy standard. In 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pages 727– 734. IEEE, 2017.

[5] Sang-hyun Kim, Dong-hwi Kim, Hyeung-seok Oh, Hyun-sig Jeon, and Hyun-ju Park. The data collection solution based on mqtt for stable iot platforms. Journal of the Korea Institute of Information and Communica- tion Engineering, 20(4):728–738, 2016.

[6] Roberto Minerva, Abyi Biru, and Domenico Rotondi. Towards a definition of the internet of things (iot). IEEE Internet Initiative, 1(1):1–86, 2015.

[7] Satoshi Nakamoto and A Bitcoin. A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 2008.

[8] Ana Reyna, Cristian Mart´ın, Jaime Chen, Enrique Soler, and Manuel D´ıaz. On blockchain and its integration with iot. challenges and opportunities. Future generation computer systems, 88:173–190, 2018.

[9] Janessa Rivera and Rob van der Meulen. Gartner says 4.9 billion connected "things" will be in use in 2015. Gartner, 2014.

[10] Ovidiu Vermesan, Peter Friess, et al. Internet of things-from research and innovation to market deployment, volume 29. River publishers Aalborg, 2014.
[11] Haoyan Wu, Zhijie Li, Brian King, Zina Ben Miled, John Wassick, and Jeffrey Tazelaar. A distributed ledger for supply chain physical distribution visibility. Information, 8(4):137, 2017.
[12] Harry Halpin and Marta Piekarska. Introduction to security and privacy onthe blockchain. In2017 IEEE European Symposium on Security and PrivacyWorkshops (EuroS&PW), pages 1–3. IEEE, 2017.
[13] Hany F Atlam, Ahmed Alenezi, Robert J Walters, Gary B Wills, and JoshuaDaniel. Developing an adaptive risk-based access control model for the in-ternet of things. In2017 IEEE international conference on internet of things(iThings) and IEEE green computing and communications (GreenCom) andIEEE cyber, physical and social computing (CPSCom) and ieee smart data(SmartData), pages 655–661. IEEE, 2017.
[14] Hany F Atlam and Gary B Wills. Iot security, privacy, safety and ethics. InDigital Twin Technologies and Smart Cities, pages 123–149. Springer, 2020
[15] Harry Halpin and Marta Piekarska. Introduction to security and privacy onthe blockchain. In2017 IEEE European Symposium on Security and PrivacyWorkshops (EuroS&PW), pages 1–3. IEEE, 2017.
[16] Minhaj Ahmad Khan and Khaled Salah. Iot security: Review, blockchain so-lutions, and open challenges.Future Generation Computer Systems, 82:395–411, 2018.
[17] Hany F Atlam and Gary B Wills. Intersections between iot and distributedledger. InAdvances in Computers, volume 115, pages 73–113. Elsevier,2019.
[18] Tiago M Fern´andez-Caram´es and Paula Fraga-Lamas. A review on the useof blockchain for the internet of things.Ieee Access, 6:32979–33001, 2018.
[19] Marco Conoscenti, Antonio Vetro, and Juan Carlos De Martin. Peer topeer for privacy and decentralization in the internet of things. In2017IEEE/ACM 39th International Conference on Software Engineering Com-panion (ICSE-C), pages 288–290. IEEE, 2017.
[20] Ana Reyna, Cristian Mart´ın, Jaime Chen, Enrique Soler, and Manuel D´ıaz.On blockchain and its integration with iot. challenges and opportunities.Future generation computer systems, 88:173–190, 2018.
[21] Hitesh Malviya. How blockchain will defend iot.Available at SSRN2883711, 2016.
[22] Oladayo Bello and Sherali Zeadally. Communication issues in the internetof things (iot). InNext-Generation Wireless Technologies, pages 189–219.Springer, 2013.
[23] Irena Bojanova, George Hurlburt, and Jeffrey Voas. Imagineering an internetof anything.Computer, 47(6):72–77, 2014.
[24] Grant Blank, Gillian Bolsover, and Elizabeth Dubois. A new privacy para-dox: Young people and privacy on social network sites. InPrepared for theAnnual Meeting of the American Sociological Association, volume 17, 2014.