JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Navigating the Intersection of Blockchain and IoT: Overcoming Hurdles and Crafting Solutions

Gurdeep kaur
Assistant professor,
GSSDGS khalsa college Patiala

Jaspreet Kaur
Assistant professor,
GSSDGS khalsa college patiala

ABSTRACT

The Internet of Things (IoT) technology has become a crucial component of daily life because it makes it easier to manage and keep an eye on processes, things, and how people interact with the physical environment. IoT is expanding exponentially in both research and business, yet it still has privacy and security flaws. IoT has some challenges that are related with security risks, such as lack of fault tolerance, inability to recognize malicious wireless sensor network (WSN) nodes, inadequate node authorization and authentication, and the insecure management of received data from IoT devices etc. The majority of the current approaches are based on centralized systems, easily hackable ecosystems, and lack of documentation addressing the traceability of sensor data In this paper, we go over the main issues and challenges with IoT data protection. Secondly, we give a quick overvi ew of blockchain technology, evaluate some of the most significant problems fix with integrating IoT and blockcha in technologies, and offer solutions and Blockchain Based IoT Integrated Framework that may be able to address the shortcomings of both IoT and blockch ain technologies.

Keywords: IOT, Blockchain Framework, WSN, Smart Contracts.

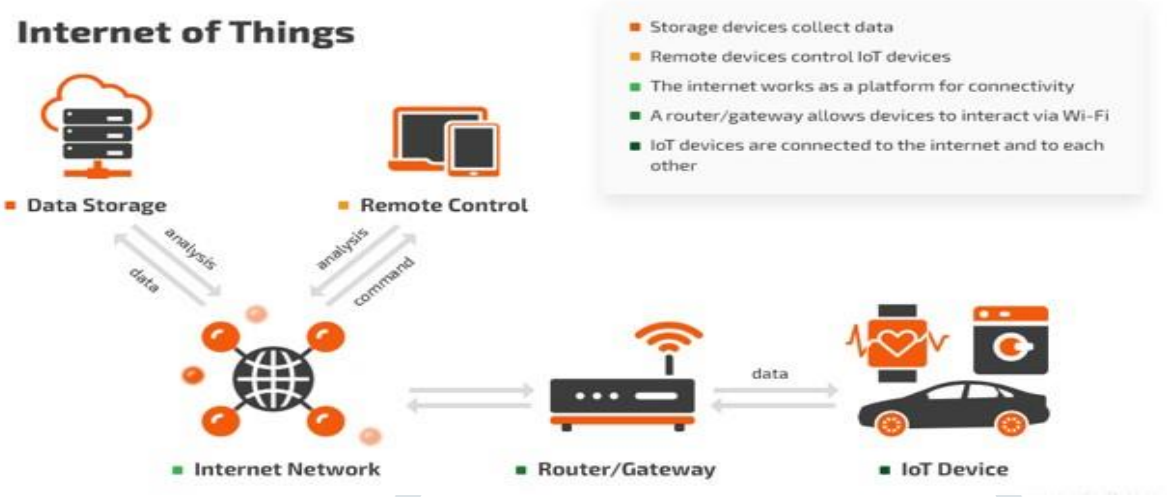
1. Introduction

Every facet of our everyday lives, including the cities we live in, the cars we drive, how we take care of ourselves, h ow we buy, how we work, and more, have been impacted by IoT.IOT is not just the future ;it is now everywhere[1].You can find sensors everywhere you look that can measure, detect, and communicate data in various ways.Despite its functionality and widespread use, I nternet of Things technology faces numerous challenges and issues with IoT device security. Today's IoT systems link to cloud servers through the Internet and rely on a centralize design[2]. This paper provides an outline of a fra mework that will leverage blockchain, a decentralized technology, for the regulation of IoT device access. Great tra nsparency, greater security, improved traceability, high efficiency, low costs, and no thirdparty involvement config uration are the primary advantages of the blockchain.

2.Why does IoT need a blockchain?

The Internet of Things (IoT) ecosystem is made up of webenabled smart devices that use embedded systems, such a s processors, sensors, and communication devices, to get, send, and act on the data they get from their surroundings [3]. By connecting to an IoT gateway or other edge device, which either sends data to the cloud for analysis or anal yses it locally, IoT devices exchange the sensor data they collect. Although individuals can connect with the device s to set them up, give them instructions, or retrieve the data, but devices accomplish the majority of the job without

their help. The development of wireless communication technologies, the miniaturisation of processing components , and the expanding accessibility of internet connectivity have all contributed to the development of the Internet of Things [4].



.

2.1 ISSUES

IoT-related problems, solutions, and applications keep emerging. IoT cannot be entirely trusted outside of the domain of the data owner since it is impossible to confirm that data has not been altered before being shared, sold, or utilized by other parties for their own gain. For example, autonomous car startups and ride sharing giants such as Uber or Ola have no solution to share trusted mapping or ride data. Instead, they gather and store similar datasets independently in their servers. So do the requirements for their security and scaling. These two issues will be the primary challenges for IoT development during the next years, predicts Gartner[5]. Security is one of the major obstacles to IoT adoption. IoT devices are frequently made to be simple to operate and connect to the internet, but this might also leave them open to hacker attacks. These are a few IoT security concerns:

These are the major challenges that blockchain technology can fix:

- W**eakauthentication:** Many IoT employ easy authentication, this kind of protection is easily breached. There are countless hacking tools and frameworks available to help an attacker guess a password through an automated sequence of attempts.
- **Unsecure connection:**
  Many IoT data leaks are caused by weak security measures used during data transmission between IoT devic es or IoT and the cloud, or during data storage on a device or in the cloud.
- **Physical intrusion.** It's possible that the hackers will change the configuration of the IoT device, for instance, when they need to record video, listen in on conversations, or launch DDoS attacks.
- **Lack of encryption:**
  Certain Internet of Things (IoT) devices do not encrypt data being transferred over the internet, which makes i t simple for hackers to intercept and steal private data.
- **Vulnerabilities in software:**
  Many Internet of Things (IoT) devices use old or insecure software that hackers can simply use to access the device or the network it is attached to..
- **Physical security:**
  Attackers having physical access to IoT devices can modify them or put malicious software on them.
- **Lack of data privacy processes:**
  Certain Internet of Things (IoT) apps need personal user devices like phones, laptop cameras, and microphone s to be a part of the ecosystem and capture users' personal data (or end-customers).

- **Complexity because of enormous data volumes**:

  By 2025, it is predicted that IoT mobile devices would produce 79.4 zettabytes of data. Given the enormous n umber of networked devices present in an IoT ecosystem, this is not surprising. Largescale data processing, tr ansmission, and storage present significant challenges.
- **Incompatibility with IoT devices and apps:**
  The architecture and protocols of the devices in an IoT network vary as well because they are made by variou s brands and are of various types. It can occasionally be difficult to guarantee that every gadget is compatible with IoT sensors. Compatibility problems exacerbate the difficulties presented by data complexity.

3.Integration With Blockchain

An internet of things architecture that is decentralised [6]. With stronger code development standards, training, thre at analysis, and testing, software development companies need to be better at implementing framework that is stable , resilient, and trustworthy at the application level. It is crucial to establish an accepted interoperability standard that is valid and safe as systems interact with one another. Without a strong bottomtop structure, every new IoT gadget will increase the dangers already present. What is required an IoT that is safeguarded for privacy and is secure. Tha t is a difficult tradeoff, but it is not impossible, and the key is to adhere to best practises while designing and imple menting blockchainIoT technology applications.Several of the security issues IoT networks are facing could be solv ed by using blockchain technology[7].Blockchain is a distributed, decentralised ledger technology that makes it pos sible to record and verify transactions in a secure and open way. Because information will be sent in the form of sec ured, signed transactions that must be recorded in a ledger distributed across each node, blockchain technology is th e most suitable method to control communication between devices in such a network [8].By merging blockchain wi th IoT, IoT networks' security and privacy can be enhanced. Each device functions as an independent node in the ne twork due to a decentralised setup technique. To collect such messages, an attacker would need to get access to all d evices, not just the central server.

3.1 This approach provides the following benefits and properties of device interaction in a distributed network :

Data decentralization:

IoT data is frequently controlled and maintained by centralised servers, opening the door for third parties to hack in to the private information. As a result of the blockchain's decentralised structure, which takes into account the absen ce of a centralised data storage and control point, there are no single sources of vulnerability[9]. Even with clouds, t he blockchain network is run by numerous separate locations, thus there is no single entity in charge of the vast maj ority of the data produced by IoT devices. Single points of failure would be eliminated by this decentralised strategy, strengthening the device ecosystem.

Identification:

A decentralised and secure system for managing IoT device identities can be made using blockchain. This could aid in guarding against unwanted access to systems and networks. The secret key of the transmitting node is used to si gn transactions between nodes, and the receiving node verifies the signature to ensure security and identification. A ny number of devices may join the network at any time and obtain a copy of the most recent distributed ledger, guar anteeing network flexibility [10].

Secure updating:

As they can safely transmit the code on the IoT devices, developers are now able to address difficulties with out-of date IoT software due to blockchains' greater safety and secure procedures.The University of Tulsa staff successfully tested this by using the opensource blockchain to update the ESP8266 firmware over a Wi-Fi connection[11].

Enhanced privacy:

Even the connection between the devices can be hidden by the blockchain, which also provides transaction validati on without the use of a third party. Moreover, the blockchain can provide the encryption and enhance the IoT proto cols. As a result, there are less chances of data leaks and IoT network hacks. Blockchains' encryption algorithms wo uld increase the privacy of customer data.

Enhanced data management:

IoT networks convey massive amounts of data in real time over many platforms, systems, and devices, creating ne w issues for data management. The blockchain enables direct data movement between devices without the need of a

server, cloud, or local database[12]. This minimize the number of transactions (device — other device — server / cloud — local network — device). In addition, the majority of interactions between IoT devices can automate smart contracts .

Enhanced scaling:

The workload is distributed among decentralised blockchain networks, resulting in better transaction processing and better coordination between the billions of IoT devices that are connected to them. Scalability is further aided by the data's ability to be shared.

Stricter authentication:

Many blockchain applications employ a decentralised PKI strategy that creates hidden and open keys to identify users. Using this method, unlike centralised PKIs, For personality identification only user has the concealed key, while the network provider receives the open key.As a result the security measures are significantly more sophisticated[13]. Both keys cannot be compromised because they are cryptographically produced.

Smart contracts:

Through the use of smart contracts, blockchain technology enables the automatic execution of IoT orders and communications[14].This can aid in the automation and streamlining of IoT operations while making sure that everyone involved is held accountable. IoT devices employ these computer algorithms for data analysis,and daily temperature measurement. The other illustration is the automatic completion of customs forms or automatic payment of duty after crossing the border[15].

Reliability of Information:

The distributed ledger blocks, which will only contain transactions validated by miners or vice versa and which will contain device output data, are what give the network's data its reliability[16].

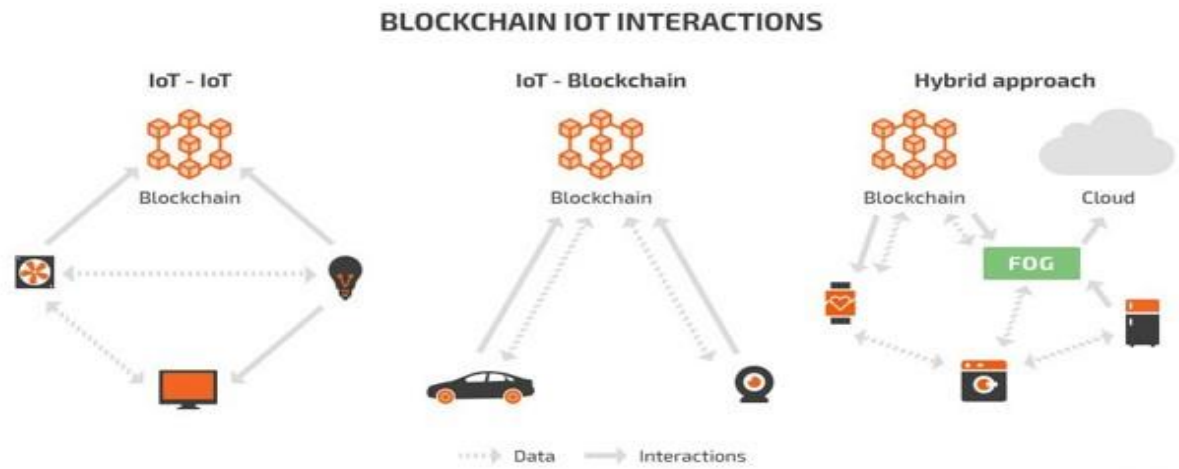
4. Blockchain Based IoT Integrated Framework?

By integrating and securing data, the blockchain IoT architecture can save costs and complexity while protecting organization investment. Collect and manage data to build a platform that is standards-based, scalable, and secure [17].

• Evaluate data and take action by separating data's business value and doing something with it.
: • Guarantee the integrity of sensing data;
• It offers capabilities common to IoT systems, enabling real-time observation and control between the user and the device.
• User interface portal with widgets for managing workload (Case View, Task Lists) and login.

4.1 How to apply blockchain technology in an IoT network

You must think about how an IoT architecture built on blockchain would interact before implementing it. You have three different ways here.



IoT — IOT:-

Since it merely requires for the use of a shared register for IoT data storage, this is actually the simplest method of integrating blockchain into the IoT network. The data will be transferred outside of the blockchain utilising a variety of routing techniques. As a result, there will be less delays and faster transaction speeds. This method also gives the devices the option of working offline. This is an easy solution to install since it does not require significant changes to the workflow of the IoT devices[18]. All that needs to be done is set up for the data to be transmitted, stored, and extracted from blockchain rather than a cloud or a server.

IoT — blockchain:-

In this method, IoT devices will communicate with each other via the blockchain, which functions as a cloud for conventional IoT networks. According to one perspective, this will improve tracing, communication security, workflow automation, and capacity[19]. If the blockchain is not quick enough, on the other hand, it will complicate the system significantly, which will lead to delays.The integration of this blockchain into IoT networks is challenging because it necessitates numerous adjustments to both the operation of IoT devices and blockchain development. A suitable blockchain should be employed as well, one with greater operating speed, capacity, and no fees. This blockchain may be powered by IOTA, Modum.io, or Riddle & Code.

Hybrid approach:-

In this scenario, the IoT devices share the majority of the data and interactions, with the blockchain merely storing specific sorts of data. There are many benefits to this, but it is very difficult to implement low latency and high operating speeds for IoT devices in real-
time.Also, this strategy aids in the introduction of fog computing to make up for the limitations of blockchains and IoT devices[20]. By using peripheral devices instead of the cloud, you may, for instance, employ this computing technique to harvest, store, and analyse private data to reduce operational costs.

Conclusion

The cloud model's centralised architecture runs the risk of having a single point of failure, excessive expenses, and latency. Blockchain technologies provide a new security architecture and protocol. Peer to peer and decentralized network architectures exhibit high levels of security, dependability, network adaptability, and the capacity for autonomous operation of their constituent elements Ultimately, the adoption of blockchain in IoT has the potential to build networks that are more reliable, accountable, and effective. It is crucial to remember that putting blockchain solutions into practise can be challenging and calls for meticulous preparation and implementation. Adoption of this technology is plagued by challenges such as limited Internet of Things resources, poor encryption, scaling concerns, and communication strategies that focus on both IoT devices and blockchain.

References

[1] P. Lade, R. Ghosh, and S. Srinivasan, "Manufacturing Analytics and Industrial Internet of Things," *IEEE Intelligent Systems*, vol. 32, no. 3,pp. 74–79, May 2017.

[2] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "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)*, March 2017, pp. 618–623.

[3] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, Jul 2017. [Online]. Available: https://doi.org/10.1007/s12083-016-0456-1

[4] M. Conoscenti, A. Vetr `o, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Nov 2016, pp. 1–6.

[5] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet-of-things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149 – 160, 2018.

[6] A. Reyna, C. Martn, J. Chen, E. Soler, and M. Daz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173 – 190, 2018.

[7] Ž. Turk and R. Klinc, "Potentials of blockchain technology for construction management," *Procedia Eng*, vol. 196, pp. 638–645, 2017.

[8] M. H. Joo, Y. Nishikawa, and K. Dandapani, "Cryptocurrency, a successful application of blockchaintechnology," *Managerial Finance*, 2019.
[9] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*, 2018, pp. 1–6.
[10] W. Nowiński and M. Kozma, "How can blockchain technology disrupt the existing business models?,"*Entrepreneurial Business and Economics Review*, vol. 5, no. 3, pp. 173–188, 2017.
[11] R. Cole, M. Stevenson, and J. Aitken, "Blockchain technology: implications for operations and supply chain management," *Supply Chain Management: An International Journal*, 2019.
[12] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Mathematical foundations of computing*, vol. 1, no. 2, p. 121, 2018.
[13] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldύ, "The rise of blockchain technology in agriculture and food supply chains," *Trends Food Sci Technol*, vol. 91, pp. 640–652, 2019.
[14] H. Hou, "The application of blockchain technology in E-government in China," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, 2017, pp. 1–4.
[15] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Appl Energy*, vol. 195, pp. 234–246, 2017.
[16]F. Allon, "Money after Blockchain: gold, decentralised politics and the new libertarianism," *Aust FemStud*, vol. 33, no. 96, pp. 223–243, 2018.

[17] G. Albeanu, "Blockchain technology and education," in *The 12th International Conference on VirtualLearning ICVL*, 2017, pp. 271–275.

[18] S. Santoso, E. P. Harahap, A. Khoirunisa, and K. Zelina, "A Systematic Review Through Intellectual Based Blockchain-Intermediary," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 2021, pp. 1–7.
[19] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," in *2018 International Conference on Information Networking (ICOIN)*, 2018, pp. 473–475.
[20] D. Dujak and D. Sajter, "Blockchain applications in supply chain," in *SMART supply network*, Springer, 2019, pp. 21–46.