




Blockchain Enabled Internet of Things: Current Scenario and Open Challenges for Future

Sanskar Srivastava¹, Anshu², Rohit Bansal³, Gulshan Soni⁴,
and Amit Kumar Tyagi⁵ 

¹ School of Computer Science and Engineering, Vellore Institute of Technology,
Chennai 600127, Tamilnadu, India

Sanskar.srivastava2020@vitstudent.ac.in

² Faculty of Management and Commerce (FOMC), Baba Mastnath University, Asthal Bohar,
Rohtak, India

³ Department of Management Studies, Vaish College of Engineering, Rohtak, India

⁴ Department of Computer Science and Engineering, School of Engineering, O.P. Jindal
University, Raigarh, Chhattisgarh, India

⁵ Department of Fashion Technology, National Institute of Fashion Technology, New Delhi,
India

amitkrtyagi025@gmail.com

Abstract. The modern world and its rapid progression have cemented the requirement of digitization and has started a revolution for automation. The fore runner for this is IoT or the Internet of Things. On a very basic level IoT can be explained as the interconnection of smart devices. The Internet of Things (IoT) describes the network of physical objects “things” that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025. IoT is quickly becoming one of the most important technologies as it allows us to connect everyday objects to the internet using embedded devices and can then be used to communicate with them. This forms a connection between the physical and digital world. But along with this huge advantage comes a lack of intrinsic security measures which make this more vulnerable and open to privacy as well as security threats. To overcome this weakness technologies such as big data and cloud computing have been tried in tandem with IoT which has provided average results. Blockchain is a system of recording data such that it becomes almost impossible to change it. It is a digital ledger of transactions that is duplicated and distributed across the entire network of computers. So, in a sense it allows us to record digitized data and distribute it but not edit it. Thus, most of the issues related to security and vulnerability can be solved quite easily. By integrating these technologies, it brings availability, security, and integrity to the applications. This research paper targets readers who have not been particularly invested in these topics and would like an overview of IoT, blockchain and their applications, uses and future prospects.

Keywords: Internet of Things (IoT) · Blockchain · Blockchain Enabled Internet of Things (BIOI) · Transactions · Nodes

1 Introduction

Now a days all major technologies focus on increasing access to electronic devices with a particular focus on wireless communication and its miniaturization. Over the years this rapid introduction has increased the number of such electronic devices resulting in better and improved services and a reduced cost making it more available and feasible for people to own. This influx of devices has changed the way people communicate and interact with each other and the environment around them. The modern world now deals with the digital world more than the real world. So, technologies were developed to better understand this new digital world. Technologies like the Wireless Sensors Network and Radio Frequency Identification has birthed IoT that provides a way to interact freely by creating a network of intelligent objects which converts the physical world into a well-connected information system. It was coined by Kevin Ashton in 1999 and has come far way since then. It has become one of the most powerful tools for business development. It is the corner stone on which the digital services are built upon and has integrated with various other technologies such as cloud computing, big data and machine learning. Devices range from wearable to hardware development [1].

IoT platforms are present in domains such as supply chain, manufacturing and energy. A platform is a mass of IoT objects which are controlled by a central node. This is an example of a centralized architecture but it also increases the chances of single point failure. Also, it requires heavy computing sources for the centralized system to collect and manage all the data collected by these objects. Issues such as data security and privacy have no standard solutions and this further complicates the management process. This variety of standards raises several problems such as flexibility, lack of scalability etc. This is where blockchain comes in as a way to combat the centralized nature. Blockchain is a decentralized immutable distributed ledger of transactions maintained by a peer-to-peer network. Instead of relying on a third party a decision must be reached by all the network participants to make any transaction acceptable. By providing a duplicate of all transaction which have taken place to all the participants it maintains data transparency and ensures high availability [2]. Third party intermediaries usually cause a delay in transaction and by eliminating the need for their involvement participants can perform transactions and share data without having to trust each other. On their own these technologies have brought improvement in various important sectors where they have been applied. By storing the sensor data and IoT objects as transactions in blockchain it creates an immutable trail of observations. All these interactions between devices in IoT smart network are stored in these immutable transactions. Blockchain relies on cryptographic hash functions and by using this feature to store transactions into blocks and linking them to each previous block in the chain it becomes almost impossible to change any previous block without being noticed. This serves various purposes, once we know the block has been linked, we can easily confirm that the interaction between nodes is securely recorded and have not been changed. Storing data hashes ensures the integrity of the data. This can be verified by comparing the hash with hash value stored into the blockchain. We will aim to understand more about how these blockchains work later on. Analysing the current cases of IoT and blockchain integration will help us understand the advantages and also bring to our attention the various challenges that come with using the newer systems. We will evaluate the working of these systems and

provide suggestions for its improvement. We will focus a little on how the BIoT can be improved and the scope it may have in the future.

2 Internet of Things - Background

Internet of Things is something which has grown in use and popularity rapidly over the last few years and its influence can be seen in areas such as smart homes, wearable devices, transportation, healthcare among other things. It is this ability which gives us a way to interconnect physical devices to communicate with other devices through the network which is so valuable. To understand the basics and how IoT works we need to know the components involved. These are sensors/devices, connectivity, data processing and user interface [3–6].

- **Sensors/devices:** This is a device which will collect data from the environment. For better understanding let us take an example. Imagine a greenhouse which has to be at a certain temperature for the proper growth of the plants. In this case the device which measures and records the temperature would count as a sensor/device.
- **Connectivity:** The data that is collected is now sent to the cloud via cellular, satellite, Wi-Fi or any other mode. Depending on the IoT application different methods can be chosen to manage the consumptions, range and bandwidth. The temperature which is recorded will be periodically sent to the cloud.
- **Data processing:** Once this data reaches the cloud the software will take care of the further processes. It will compare all the temperature reading and check whether it is within the suitable range for maximum plant growth.
- **User interface:** Now after the comparison is complete this final data has to be presented to the user via e-mail or text. In this case if the temperature is too high or low then the manager will receive a text informing him of the malfunction which he can now fix either manually or through an app which helps him regulate the temperature. Instead of the user interacting after the alert he could also have pre = defined some rules which would then automatically adjust the temperature.

This is how the basic model of IoT works. Current IoT using applications mostly use a centralized server-client cloud architecture. But peer-to-peer wireless sensor networks are also being used to handle the shortcomings of the centralized systems. The main challenges faced are:

- **Privacy and security:** The main issue arises due to the connectivity component of IoT which allows an entrance to hackers and other malpractices to take place. Older models are more susceptible to attacks as most of these systems weren't originally build to handle the connectivity between devices. As seen from the example given the device/sensor plays a major role, we have only taken one simple device to explain how IoT works but most smart environments would contain multiple devices which communicate with each other. Each node here is a point of failure which can be used to hack into the system or launch cyber-attacks. This can cause the collapse of the entire system.

- Hardware: Choosing the correct devices and sensors which will ensure that data will be collected and transferred safely has to be done carefully.
- Data management: The data collected and transferred by the devices are massive and the need to manage it requires a lot of computing power and efficient use of data pipelines for the processing. Machine learning and predictive analysis can be used to make this easier.
- Device maintenance: The smart devices have to be regularly checked to make sure they are functioning and providing accurate data.
- Infrastructure: Cloud computing, fog computing etc. are on of the many types of architectures available and have to be chosen accordingly (refer Fig. 1).

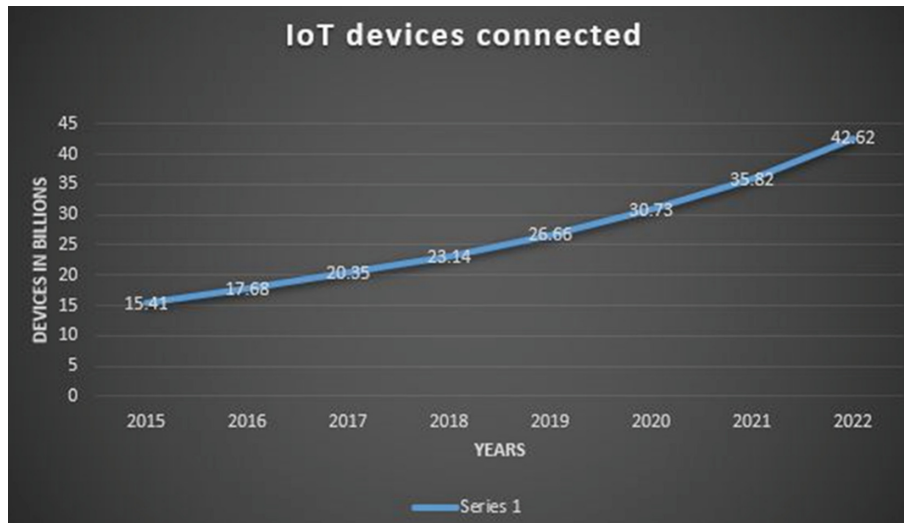


Fig. 1. Status of IoT devices in current era

3 Blockchain

Satoshi Nakamoto introduced the concept of a decentralized peer-to-peer electronic cash system when he published a paper on Bitcoin. This new data structure which could be used for transactions and validations was named blockchain [7].

Bitcoin used blockchain technology for all the online trading which was free and available to everyone all around the world without the need of a third-party intermediary. After coming to know the various features such as security, privacy, integrity, immutability, fault tolerance etc. it became popular in other sectors such as agriculture, smart grids, healthcare, supply chain management and many more. In recent years it has become one of the most widely researched topics. It provides a distributed, immutable secure ledger of transactions. The blockchain protocol constructs a chain of block with

each block containing a set of transactions at a particular time. New block is linked to the previous blocks using a reference hence the term ‘chain’. The four main components involved in a blockchain are:

- Peer-to-peer network: This aims to remove the centralization present by providing all the nodes the same privileges and enable easier interaction amongst the nodes. This is done through the use of the private and public keys. The private key is used for decryption and signing transactions while the private key is used for encrypting and to provide an address for the network to reach.
- Ledger: the ledger is used for recording all the transactions performed in order. This information is duplicated and made available to all the nodes. The ledger itself is open and everyone on that network can view it. Each node can then decide the validity of the transaction.
- Synchronization: To synchronize the ledgers of the nodes we have to broadcast all the transactions, validate them and add the validated transactions again to the ledger.
- Miners: due to delays all nodes may not receive the blocks of transactions at the same moment thus to prevent every node from adding a transaction (to maintain the valid and ordered branch) unique nodes which can add transactions called miners are used. The miner needs to compete with other minors to make a new transaction and validate it.

Each block is a set of instructions which include a Header and the block content. The Header contains the timestamp, difficulty target, hash value of previous header for the chain creation, encoded transaction into a single hash code and nonce. The block content contains all the information about the data itself (input and output). The input of a current block contains the output of the previous transaction and a field containing the signature with the private key which validates the ownership. The output contains the data to be sent and address/public key of the receiver. Since only the private key of the receiver can prove ownership only that particular receiver can handle the data. This makes sure that no tampering can take place making it secure and distributed [8]. To avoid double spending attacks and to maintain integrity consensus mechanism is utilized. The end goal here is to reach a consensus in the network where third-party involvement is not required and participants need no trust one another. Selecting a leader who validates the new block and then propagates it to the network. This validation takes place when a majority of nodes find a block acceptable so it can then be added to the network [9].

4 Integration of IoT and Blockchain (BIoT)

Now that we have a basic overview of how IoT and blockchain works we can see the need of blockchain to fix the various issues that IoT currently possesses. IoT issues like reliability and privacy are easily solved if we use blockchain. The single point of failure is also resolved due to its distributive nature. The Trusted IoT alliance was formed in 2016 to make IoT more fluid and reliable by merging blockchain technology into the IoT framework. Many other projects that aim to do the same were started like Linux Foundation’s Hyperledger Project, LO3ENERGY, IoTex, Raspnode etc. The improvements that BIoT has experienced are as follows [10–12]:

- Decentralization and scalability: peer-to-peer removes central points of failures, improved fault tolerance and system scalability.
- Identity: participants in the BIoT can identify every device which is being used. Since the data recorded is immutable it can be trusted to be authenticated. Improves the IoT field and the participants.
- Autonomy: using BIoT enables devices to interact without any involvement of the servers. This encourages development of smart autonomous hardware.
- Reliability: Participants are capable of verifying the authenticity to be certain that no tampering has taken place. It also enables the data traceability.
- Security: communication and interaction between the devices can be stored as transaction of the blockchain. These can also be validated as smart contracts to secure communication.
- Marketing: BIoT improves the time it takes to create an IoT system and environment. Services can be easily deployed and payments can be done easily and securely. This improves the overall interconnection.

5 Blockchain Enabled Internet of Things (BIoT) Architecture and Interactions

There are many hybrid designs created for better integration between IoT and blockchain [13].

- IoT – IoT design: Here the transactions take place between IoT peer devices. It is utilized when low latency and fast performance is required. The data of transactions between IoT peer devices is stored in the blockchain but all the other data is transferred directly among the IoT devices. This method ensures a smooth and efficient flow of data from one device to another, it is preferable that the devices are in the same domain or network to reduce the complication which would arise during routing.
- IoT peer – to blockchain design: unlike the previous design all the IoT peer devices are not directly connected to each other. The interactions and communications are done through the blockchain. Here the blockchain can monitor and validate all the data related to the transactions that take place. This creates better transparency and traceability. Thus, data can be secure even if the devices belong to different domains. The challenge that arises here is that by recording all the transactions there is an increase in the bandwidth and data. It would also face more latency and scalability issues while also requiring more computational power to handle the nodes needed for this. Applications which focus on renting and trading utilize this design.
- Hybrid architecture design: The introduction of edge computing has improved the communication and processing of the data. This kind of hybrid design involves the use of artificial intelligence (AI), fog computing and edge computing to create a more interactive and improved environment for IoT devices. This method also causes an increase in the computational power and consumption but not at the level as the previous design which requires devices to act as nodes. It also reduces the bandwidth and latency issues. Here the heavy work is done by fog or edge computing so all blockchain interactions are done by this layer as not all the transactions of IoT peer devices directly go through the blockchain.

6 Challenges Faced in BIoT

We have seen how the technologies of IoT and blockchain complement each other to create a better improved design but there are still issues that can arise and need improvement as blockchain is designed for more powerful computers which is not feasible for IoT currently [14, 15].

- **Storage and scalability:** Blockchain currently can only process a few transactions per second and is not designed to store large amounts of data. Data produced in IoT devices is in gigabytes can create issues for the capacity present in the blockchain. Since most of the data stored is not that useful, techniques which filter and compress the data can help reduce this problem. To increase the bandwidth while reducing latency enable better transitions and can be accomplished by using consensus protocol.
- **Security:** We have extensively discussed how the inclusion of blockchain can help fix the issue with rising attacks on IoT devices and the security but this is said on the basis that the data generated by the IoT stays immutable when it arrives in the blockchain. However, if the data is already corrupted before being introduced to the blockchain then it would stay corrupt even with the help of the blockchain. Sometimes due to various reasons the devices themselves fail to work properly and give the wrong data and this issue would not be recognized until the device is tested and recalibrated. Thus, to avoid issues like this the IoT devices should be well checked regularly and also kept in the right places to avoid any physical damage. Run-time upgrading mechanisms along with methods of failure detection should be used as well. Filament is a project which functions fairly well in terms of security.
- **Data privacy:** A lot of IoT devices work with confidential data that requires data privacy and identity management. Integration of security cryptographic software would be required to ensure that data is stored properly and cannot be accessed without permission.
- **Smart contracts:** smart contracts would be an excellent method of making the recording of all interactions and transactions secure and reliable. The smart contracts need the oracles to provide real world data which has to be accurate and trusted. IoT can cause issues here since validating this would make it unstable and accessing so many diverse data sources would overload them.
- **Legal issues:** There is a need to implement control over the network. IoT is also affected by the country and its regulations related to data privacy. These laws need to be revised and updated with these new technologies in mind. This will help in standardizing many protocols for certification of security features and thus create a more trusted IoT network. This will have a major influence in the future of any integrated technology.
- **Consensus:** A lot of the consensus algorithms are beyond the current capabilities of IoT as they require more resources from the nodes. Lightweight nodes would help solve this issue but most blockchains do not support this yet. More research is required to make sure mining does not continue to be an issue.

7 Applications of BIoT

The various sectors and areas that BIoT can be applied to are [16, 17]:

- Energy sector
- Smart contract: Slock.it works with smart contracts that enable renting and trade
- Industrial IoT
- Database
- Healthcare
- Agriculture: A food traceability system was made to identify the food products as well as the parties involved in the supply of food.
- Transportation
- Smart homes and cities: Smart homes like Telstra in Australia.

7.1 Future Scope and Directions

- Machine learning for privacy and security in BIoT applications
- Fixing challenges related to decentralization
- Blockchain infrastructure which solves all the issues if BIoT implementations
- Legal issues and regulations
- Scalability is still a major issue and many researches are still going on.

8 Conclusion

This research paper was aimed toward readers who were not familiar to the newer upcoming technologies. We explained how IoT works and the issues it faces and how other technologies can be used along with it to improve its performance. One of the technologies that would help is blockchain and we have also learned how it works and how it can help IoT in fixing the issues it faces. We then combined and integrated these two technologies and discussed the improvements and the challenges that need to be addressed to fine tune this system to achieve the full potential of both technologies. Concluding we can say that the integration of blockchain and IoT is a must for advancement and to improve this further we need to analyse the main challenges and work towards fixing them. The BIoT is still in its early stages and there is a lot of room for growth and in the future, it is imperative that we merge more technologies which complement each other and introduce more applications to encourage the development in marketplaces. A more liberal and wider use of this technology will require the cooperation of stakeholders, governments and other institutions to provide the right structure to harness the power of BIoT applications.

References

1. Panarello, A., Tapas, N., Merlino, G., Longo, F., Puliafito, A.: Blockchain and IoT integration: a systematic survey. *Sensors* **18**, 2575 (2018). <https://doi.org/10.3390/s18082575>

2. Shammar, E.A., Zahary, A.T., Al-Shargabi, A.A.: A survey of IoT and blockchain integration: security perspective. *IEEE Access* **9**, 156114–156150 (2021). <https://doi.org/10.1109/ACCESS.2021.3129697>
3. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **88**, 173–190 (2018). ISSN 0167-739X. <https://doi.org/10.1016/j.future.2018.05.046>
4. Nartey, C., et al.: On blockchain and IoT integration platforms: current implementation challenges and future perspectives. *Wirel. Commun. Mob. Comput.* **2021**, Article no. 6672482, 25 p. (2021). <https://doi.org/10.1155/2021/6672482>
5. Saxena, S., Bhushan, B., Ahad, M.A.: Blockchain based solutions to secure IoT: background, integration trends and a way forward. *J. Netw. Comput. Appl.* **181**, 103050 (2021). ISSN 1084-8045. <https://doi.org/10.1016/j.jnca.2021.103050>
6. Hassan, M.U., Rehmani, M.H., Chen, J.: Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions. *Future Gener. Comput. Syst.* **97**, 512–529 (2019). ISSN 0167-739X. <https://doi.org/10.1016/j.future.2019.02.060>
7. Makhdoom, I., Abolhasan, M., Abbas, H., Ni, W.: Blockchain’s adoption in IoT: the challenges, and a way forward. *J. Netw. Comput. Appl.* **125**, 251–279 (2019). ISSN 1084–8045. <https://doi.org/10.1016/j.jnca.2018.10.019>
8. Lo, S.K., et al.: Analysis of blockchain solutions for IoT: a systematic literature review. *IEEE Access* **7**, 58822–58835 (2019). <https://doi.org/10.1109/ACCESS.2019.2914675>
9. Zafar, S., Bhatti, K.M., Shabbir, M., Hashmat, F., Akbar, A.H.: Integration of blockchain and Internet of Things: challenges and solutions. *Ann. Telecommun.* **77**, 13–32 (2022). <https://doi.org/10.1007/s12243-021-00858-8>
10. Aggarwal, V.K., et al.: Integration of blockchain and IoT (B-IoT): architecture, solutions, & future research direction. *IOP Conf. Ser. Mater. Sci. Eng.* **1022**, 012103 (2021)
11. Chen, T.-H., Lee, W.-B., Chen, H.-B., Wang, C.-L.: Revisited—the subliminal channel in blockchain and its application to IoT SECURITY. *Symmetry*. **13**(5), 855 (2021). <https://doi.org/10.3390/sym13050855>
12. Maroufi, M., Abdolee, R., Tazekand, B.M.: On the convergence of blockchain and Internet of Things (IoT) technologies. *J. Strateg. Innov. Sustain.* (2019). <https://doi.org/10.33423/jsis.v14i1.990>
13. Atlam, H.F., Azad, M.A., Alzahrani, A.G., Wills, G.: A review of Blockchain in Internet of Things and AI. *Big Data Cognit. Comput.* **4**(4), 28 (2020). <https://doi.org/10.3390/bdcc4040028>
14. Moudoud, H., Cherkaoui, S., Khoukhi, L.: Towards a scalable and trustworthy blockchain: IoT use case. In: *ICC 2021 - IEEE International Conference on Communications* (2021). <https://doi.org/10.1109/ICC42927.2021.9500535>
15. Sheth, H.S.K., Ilavarasi, A.K., Tyagi, A.K.: Deep learning, blockchain based multi-layered authentication and security architectures. In: *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, Salem, India, pp. 476–485 (2022). <https://doi.org/10.1109/ICAAIC53929.2022.9793179>
16. Deshmukh, A., Sreenath, N., Tyagi, A.K., Jathar, S.: Internet of Things based smart environment: threat analysis, open issues, and a way forward to future. In: *2022 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, pp. 1–6 (2022). <https://doi.org/10.1109/ICCCI54379.2022.9740741>
17. Tyagi, A.K., Chandrasekaran, S., Sreenath, N.: Blockchain technology:—a new technology for creating distributed and trusted computing environment. In: *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, Salem, India, pp. 1348–1354 (2022). <https://doi.org/10.1109/ICAAIC53929.2022.9792702>