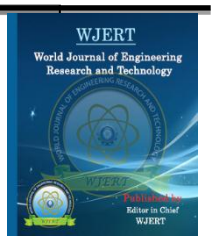
wjert, 2023, Vol. 9, Issue 7, 116-126. Review Article ISSN 2454-695X

World Journal of Engineering Research and Technology
WJERT
www.wjert.org SJIF Impact Factor: 5.924



A REVIEW ON IOT WITH BLOCK CHAIN TECHNOLOGY: ARCHITECTURE VIEW, APPLICATIONS & INTEGRATION

Dr. A. Bajulunisha* and V. Dhamodharan

M.A.M College of Engineering and Technology, Siruganur, Trichy.

Article Received on 16/05/2023 **Article Revised on 06/06/2023** **Article Accepted on 26/06/2023**

***Corresponding Author**
Dr. A. Bajulunisha
M.A.M College of Engineering and Technology, Siruganur, Trichy.

ABSTRACT

The Internet of Things (IoT) is crucial in every industry. With the addition of new functions, practically every industry now uses it. Since it is used everywhere, key security components are extremely important and must be kept. A new technology called block chain which in the last decade has influenced our lifestyles most. Bit coin is a word used frequently for Block chain. Block chain is a powerful technology that decentralizes computation and management methods that may resolve many of IoT troubles, in particular safety. We introduce IoT enabled with block chain in this article, as well as some of its major features, architecture layout, distinguishing characteristics, futuristic solutions to various real-world problems, various communicational models, etc. Both technologies have some distinguishing qualities in each area, but they also have some drawbacks, which point the way for further research.

1. INTRODUCTION

A well-known and rising technology called the Internet of Things (IoT) aims to connect all kinds of gadgets to the internet. The development of Internet of Things devices is aided by the seamless integration of Radio Frequency Identification, wireless communication, and sensors. Platforms with embedded IoT services and smart features are used to deliver smart services, integrating the physical and digital worlds through electromechanical systems and controllers. Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (Co-AP), and Bluetooth Low Energy are a few examples of IoT protocols. Numerous issues arise due to the variety of IoT standards, protocol standards, and IoT

devices, including lack of scalability, adaptability, and interoperability. Different architectural patterns, including services-oriented architectures (SOA) and micro services architecture, which are components of services-oriented solutions, are used in the design of IoT systems. The IoT devices in these systems provide service to other devices via the communication protocol. A service contract makes business functionality available as part of the service. A service contracts includes documentations, service policies, QoS, and a service interface for monitoring and ensuring the QoS and the performance of IoT transactions. The methods used for interoperability, integrations, and enabling seamless services composition among IoT platforms and applications which works on different devices over heterogeneous networking technologies is called service managements.[1]

The businesses are substantially adopting the architecture of growing Internet of Things (IOT) technology, which opens up new revenue streams for a number of businesses. IoT solutions have become more popular in the industrial sector over the past several years. Block chain, which is regarded as the most encouraging technology, is created as a result of crypto currency. The data of regular transactions which is done by large number of users and devices is stored and track by decentralized applications (DApps). From cryptocurrency DApps arises.[2] The IoT can comprehend various networks of communication where the devices could interact with each other through internet. They are commonly known as "entities" or "things" and as delineated in Fig1, they have particular characteristics that are examined underneath.

- ***Identification-*** All IoT devices require to have identification like sixth version of Internet Protocol (IPv6) address to share or exchange information with other objects.
- ***Sensing-*** To collect information, the sensing methods are used to sense physical environment.
- ***Communication-*** It means linkage methods and are exploit for communicating the objects.
- ***Computation-*** These methods are adopted to gather the data that is obtained by objects.
- ***Services-*** It refers to those methods that are given by objects in relation with information to the users that is received from the physical environment.
- ***Semantics-*** It means objects have the power to use the correct information from environment.

Examples of IoT devices include beagle board, RFID (Radio Frequency Identification) tags,

CubieBoard, Raspberry Pi, Beagle Board and Arduino.[3]

Development boards, which have a CPU, read-only memory, random access memory, and a number of analogue and digital input/output connectors, also include microcontrollers. Different sensors are often tied to MCU processing, receiving trigger, and transfer to additional systems. Potentiometers, accelerometers, temperature, vibration sensors, proximity sensors, moisture sensors, and air quality sensors are a few of the sensors. Processing data, allocating memory, and other communication-supporting utility functions all require real-time operations. RTOS is chosen based on the product's performance, functional requirements, and security. WSN, also known as a wireless sensor network, is one of the most popular IoT enabling technologies at the moment.[68,69] Designing and implementing security is a very big barrier in WSN, largely because of constrained. Numerous other uncommon features of IoT and WSN, in addition to the usual challenges faced when designing security in both IoT and WSN, demonstrate that security cases and situations in IoT are significantly more severe and complex than in WSN for the same reason—their dissimilar features and uncommonly targeted applications and systems. First off, applications designed for gathering raw data, such environmental surveillance and inspection systems, are where WSNs are most frequently used. Sensors are primarily responsible for collecting, storing, and sending all of the data. Reliable multiloop routing protocols are used to send the data to sinks. As a result, most communication is unidirectional, even if the opposite direction is also employed to transmit orders and control signals, which are then used to operate sensors. Second, the end system in the Internet of Things (IoT) and sensors both confront the issue of limited resource availability, however sensors may experience more issues with power limitations.[4]

There are a variety of systems created expressly for the decentralized functioning of the IoT.In the deployment of big-scale observation structures in remote regions, when there isn't an everlasting connection with the Internet, the community calls for disbursed storage techniques for growing the quantity of records storage which decreases the probability of statistics loss. Unlike conventional networked data storage, distributed storage is constrained via the confined assets of the sensor.[5]

Since applications and transactions that require the authentication of centralized architects and trusted third parties can now operate decentrally with the same level of certainty, Blockchains has brought severe changes to its conventional business operations. Equality

such as transparency, robustness, auditability, and safeguards are provided by blockchain architecture and design (Greenspan, 2015a; Christidis and Devetsikiotis, 2016). An output database arranged as a block list in which the committed blocks cannot be altered might be seen as a block chain. This is good for banks as banks may work together under the same blockchain to push the transactions of their clients.[6]

The later sections of the paper standardized as follows: Section 2 illustrated IoT architecture, Section 3 describes the Blockchain as a Solution for IoT, Section 4 explain Integration of Blockchain and IoT, Section 5 shows Future research directions followed by Conclusion in Section 6.

2. IoT- Architectural View

In recent years, IoT technology has grown in popularity and it has a large variety of applications. IoT applications operate according to how they have been designed based on the different application areas. However, there is no standard defined architecture of work that is strictly adhered to across the board. The complexity and number of architectural layers vary according to the specific business task at hand. Four-layer architecture is the standard and most widely accepted format.[6]

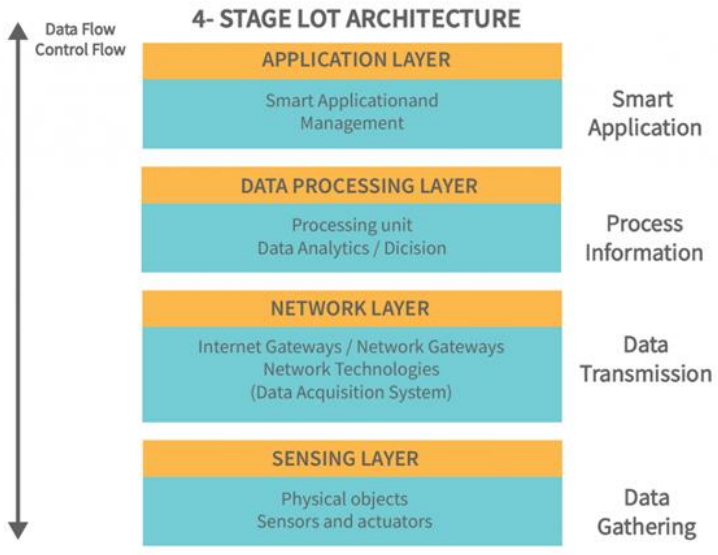


Fig. 1: IOT Architecture view.

Perception/Sensing Layer

The first layer of any IoT system involves “things” or endpoint devices that serve as a conduit between the physical and the digital worlds. Perception refers to the physical layer, which

includes sensors and actuators that are capable of collecting, accepting, and processing data over the network. Sensors and actuators can be connected either wirelessly or via wired connections. The architecture does not limit the scope of its components nor their location.

Network Layer

Network layers provide an overview of how data is moved throughout the application. This layer contains Data Acquiring Systems (DAS) and Internet/Network gateways. A DAS performs data aggregation and conversion functions (collecting and aggregating data from sensors, then converting analog data to digital data, etc.). It is necessary to transmit and process the data collected by the sensor devices. That's what the network layer does. It allows these devices to connect and communicate with other servers, smart devices, and network devices. As well, it handles all data transmissions for the devices.

Processing Layer

The processing layer is the brain of the IoT ecosystem. Typically, data is analyzed, pre-processed, and stored here before being sent to the data center, where it is accessed by software applications that both monitor and manage the data as well as prepare further actions. This is where Edge IT or edge analytics enters the picture.

Application Layer

User interaction takes place at the application layer, which delivers application-specific services to the user. An example might be a smart home application where users can turn on a coffee maker by tapping a button in an app or a dashboard that shows the status of the devices in a system. There are many ways in which the Internet of Things can be deployed such as smart cities, smart homes, and smart health.

3. Applications and Categories of IoTs

IoT has been utilized in various areas, from home to health, education, and agriculture industries. As an introduction, we highlighted the coarse evolutionary events of IoTs and different use cases. However, in this section, we instantiate major applications of IoTs under seven categories.

(i)Climate and Environmental (Aquatic/Terrestrial) IoT: Environmental IoTs are composed of sensors employed for different purposes, such as detecting pathogens, chemicals, gas, temperature, and(or) other variables in an environment, such as land or water bodies.[8] For

instance, regulatory bodies such as Environment Protection Agency (EPA) often employ IoT to monitor the risk factors that affect human and environmental health. Similarly, industries based on land and water resources have benefited from the IoTs for various business needs. For instance, climate and environmental IoTs have been used for real-time monitoring and forecasting of weather, and climatic conditions in an area.[9]

(ii)Forest and Agricultural IoT: Applying IoTs has proved profitable in forestry, and crop/animal farming.[10,11,12] Chiefly, IoT systems have been used for managing and monitoring several aspects of farming, such as irrigation, pest control, weed control, and crop density monitoring, among others.[19]

(iii)Industrial IoT: The use of IoTs has been profitable in industries of varying kinds, such as hospitals,[13] manufacturing industries, and retail and whole-shale markets, among others. Everyday use cases of an industrial IoT include remote condition monitoring, digital work instructions, predictive mainteisce, and disaster management. Using industrial IoTs brings several benefits, such as maximizing revenue, reducing time to market, and lowering operational costs.

(iv)Smart Home IoT An IoT find(s) is one of its most popular applications inside a home setting. Automating lighting, sound, and kitchen work such as cooking and washing are automated by using different connected devices. Controlling and maintaining home climate can also be performed effectively using sensors such as thermostats.[14,15,16]

(v)Wearable IoT: Wearable IoT comprises wearable technologies such as Fitbit, Holter monitor, personal alarm devices, smart watches, etc. The sensing devices have become so small that they have been integrated into normal clothing items such as bras or vests, caps, shoes, and travel/school backpacks.[16,17,18] Wearable IoT has helped monitor personal health and supports remote health services.[19]

(vi)Smart City IoT: Smart city IoTs are an extended version of the smart home IoT.[14] It comprises many sensor technologies to sense an urban environment, streets, highways, traffic, and vehicle mobility. Smart retail shopping, intelligent health services and smart parking are also an integral part of a smart.[15]

(vii)Vehicular IoT: Vehicular IoT can be considered one of the components of a smart city IoT. Sensors that collect data from terrestrial and aerial vehicular devices constitute vehicular

IoT. The data may be helpful to route the vehicular devices efficiently or may be helpful to collect environmental data such as temperature and humidity. For instance, United Parcel Service (UPS), a shipping company, deploys sensors in its transport vehicles to collect data such as mileage, speed, fuel cost, etc., for big data analysis.[21,22] Unmanned aerial vehicles (UAVs) also use different sensor data to optimize their route and operations to support "collaborative autonomous driving, and advanced transportation.[23]

4. IoT and Block chain Integration

The IoT has proven to automate domestic, industrial, and business monitoring and functioning. Nevertheless, it relies on centralized cloud computing for data storage, processing, and network command and control. With the centralized model, the integrity of the data and the process output of cloud computing are always in question because IoT owners have to rely on a third party (such as cloud vendors) for the integrity of the data and the process outputs.[30]

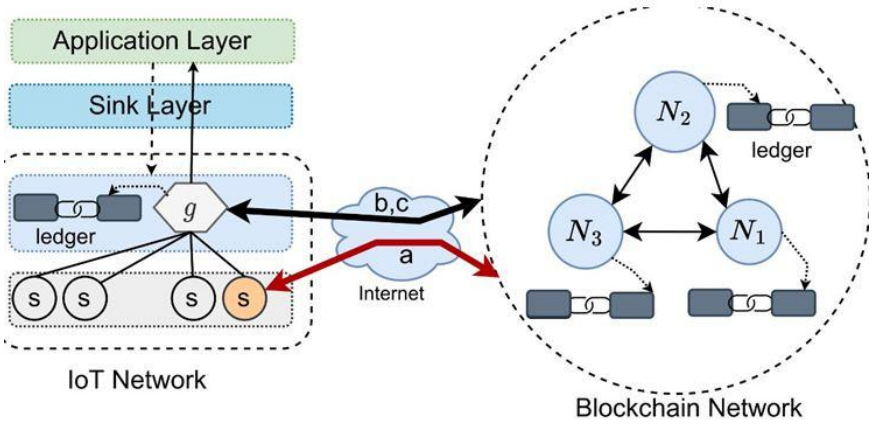
On the other hand, the basic features of a blockchain network include transparency, verifiability, data redundancy, and trustworthy.[24] These principal features can fill the gaps in providing the security-related guarantees required by an IoT network and related applications. Thus integration of an IoT and a blockchain network can serve a primary need for colossal storage, business/industry automation, fault-tolerance, and data/process integrity.

Devices in an IoT network can be designed to play different roles in a blockchain network. Edge devices such as routers, routing switches, integrated access devices, multiplexers, and gateways can be designed to store the blockchain and perform transaction validations. Intermediate devices such as relay routers can be designed to execute services for issuing transactions to a BCN on behalf of the connected resource constraint devices such as sensors. Several integration models have been discussed in previous studies.[25,26] Nevertheless, we summarize them into four major IoT and BCN integration models.

1. Sensor devices as Transaction Issuer (SaTi): In this integration model (see the interaction (a) between sensor node *s* and BCN in Figure 2), IoT devices such as sensors take part in issuing transactions to the external BCN. Such IoT devices should be designed to accommodate computational power and bandwidth requirements. However, the typical IoT devices do not have the storage capacity to store a complete blockchain. In many use cases, such as industrial IOTs, this model may be too costly and ineffective for sensors to communicate with an external BCN. In that case, edge devices such as IoT gateways may be

employed to issue transactions on behalf of all the low-power, resource constraint IoT devices.

2. Edge devices as Transaction Issuer (EaTi): In this integration model (see the interaction (b) between edge device *g* and BCN in Figure 6), specially designed IoT edge devices such as gateway routers may be actively issuing transactions to an external BCN, without actually storing a copy of the blockchain ledger. This integration model is efficient, given that it requires a limited number of edge devices for interacting with the BCN.



3. Edge devices as Transaction Verifier (EaTv): This integration model extends the EaTi model, where specially designed IoT edge devices issue transactions to the BCN and maintain an entire block chain ledger for active block validations. In many cases, edge devices could handle both issues and validate transactions being an active node for a BCN. However, unless business interests require it, an industry may not use edge devices for transaction validations, which are computationally intensive and require higher storage and bandwidth. In the figure, interaction (c) is part of this integration model.

4. Hybrid: In a hybrid integration model, IoT and block chain interact through edge devices and specially designed IoT sensor devices. It depends on the applications whose interactions go through edge and IoT devices. In the figure, interactions (a), (b), and (c) are part of the hybrid integration model. In other words, sensor devices issue transactions, and edge devices issue, and validate transactions for a BCN. Nonetheless, this model imposes redundancy in issuing transactions for a BCN, which is costly in terms of bandwidth.

REFERENCES

1. Nikoukar, A., Raza, S., Poole, A., Gunes, M., & Dezfouli, B. Low-power wireless for the internet of things: Standards and applications. IEEE Access, 2018; 6: 67893–67926. https://doi.org/ 10.1109/access.2018.2879189.
2. Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. IEEE Transactions on Industrial Informatics, 2018; 14(11): 4724– 4734. https://doi.org/10.1109/tii.2018.2852491.
3. Fan, K., Luo, Q., Zhang, K., & Yang, Y. Cloud-based lightweight secure RFID mutual authentication protocol in IoT. Information Sciences, 2020; 527: 329–340. https://doi.org/10.1016/j. ins.2019.08.006.
4. Chowdhury, A., & Raut, S. A. A survey study on internet of things resource management. Journal of Network and Computer Applications, 2018; 120: 42–60. https://doi.org/10.1016/j. jnca.2018.07.007.
5. Taheri, Negar, ShahramJamali, and Mohammad Esmaeili. "Achieving Performability and Reliability of Data Storage in the Internet of Things, 2022.
6. Angotu Saida, R.K.Yadav. Review on: Analysis of an IoT Based Blockchain Technology" I. J. Education and Management Engineering, 2022; 2: 30-37. DOI: 10.5815/ijeme.2022.02.04.
7. Narash Adhikari, Mahalingam ramkumar,"IoT and Blockchain Integration: Applications, Opportunities and Challenges" *Network*, 2023; *3*(1): 115-141. https://doi.org/10.3390 /network3010006.
8. McGrath, M.J.; Scanaill, C.N. *Sensor Technologies—Healthcare, Wellness and Environmental Applications*; Apress: Berkeley, CA, USA, 2013; 1–302. [Google Scholar] [CrossRef]
9. Ahire, D.B.; Gond, D.V.J.; Ahire, N.L. IoT Based Real-Time Monitoring of Meteorological Data: A Review. In Proceedings of the 3rd International Conference on Contents, Computing & Communication (ICCCC-2022), Nashik, India, 2022; 1–12. [Google Scholar] [CrossRef]
10. Dineva, K.; Atanasova, T. Design of Salable IoT Architecture based on AWS for Smart Livestock. *Animal*, 2021; *11*: 2697. [Google Scholar] [CrossRef] [PubMed]
11. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access*, 2020; *8*: 34564–34584. [Google Scholar] [CrossRef]

12. Sontowski, S.; Gupta, M.; Laya Chukkapalli, S.S.; Abdelsalam, M.; Mittal, S.; Joshi, A.; Sandhu, R. Cyber Attacks on Smart Farming Infrastructure. In Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing, CIC 2020, Virtual, 1–3 December 2020; Institute of Electrical and Electronics Engineers Inc.: Interlaken, Switzerland, 2020; 135–143. [Google Scholar] [CrossRef]
13. YIN, Y.; Zeng, Y.; Chen, X.; Fan, Y. The internet of things in healthcare: An overview. *J. Ind. Inf. Integr*, 2016; *1*: 3–13. [Google Scholar] [CrossRef]
14. Ainane, N.; Ouzzif, M.; Bouragba, K. Data security of smart cities. In Proceedings of the 3rd International Conference on Smart City Applications, Tetouan, Morocco, 10–11 October 2018. [Google Scholar] [CrossRef]
15. Ibrahim, J.M.; Karami, A.; Jafari, F. A secure smart home using Internet-of-Things. In Proceedings of the 9th International Conference on Information Management and Engineering, Barcelona, Spain, 2017; 69–74. [Google Scholar] [CrossRef]
16. McGrath, M.J.; Scanaill, C.N. *Sensor Technologies—Healthcare, Wellness and Environmental Applications*; Apress: Berkeley, CA, USA, 2013; 1–302. [Google Scholar] [CrossRef]
17. Mann, S. Historical account of the 'WearComp' and 'WearCam' inventions developed for applications in 'personal imaging'. In Proceedings of the International Symposium on Wearable Computers, Digest of Papers, Cambridge, MA, USA, 1997; 66–73. [Google Scholar] [CrossRef]
18. Tariq, N.; Qamar, A.; Asim, M.; Khan, F.A. Blockchain and smart healthcare security: A survey. In *Procedia Computer Science*; Elsevier: Amsterdam, The Netherlands, 2020; 175: 615–620. [Google Scholar] [CrossRef]
19. Arunkumar, N.; Pandimurugan, V.; Hema, M.S.; Azath, H.; Hariharasitaraman, S.; Thilagaraj, M.; Govindan, P. A Versatile and Ubiquitous IoT-Based Smart Metabolic and Immune Monitoring System. *Comput. Intell. Neurosci*, 2022; *2022*: 9441357. [Google Scholar] [CrossRef] [PubMed]
20. Ainane, N.; Ouzzif, M.; Bouragba, K. Data security of smart cities. In Proceedings of the 3rd International Conference on Smart City Applications, Tetouan, Morocco, 10–11 October 2018. [Google Scholar] [CrossRef]
21. Chao, H.; Maheshwari, A.; Sudarsanan, V.; Tamaskar, S.; Delaurentis, D.A. UAV traffic information exchange network. In Proceedings of the 2018 Aviation Technology, Integration, and Operations Conference, Atlanta, GA, USA, 2018. [Google Scholar] [CrossRef]

22. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE internet Things J.*, 2017; *4*: 642–646. [Google Scholar] [CrossRef]
23. Peng, C.; Wu, C.; Gao, L.; Zhang, J.; Yau, K.L.A.; Ji, Y. Blockchain for Vehicular internet of Things: Recent Advances and Open Issues. *Sensors*, 2020; *20*: 5079. [Google Scholar] [CrossRef] [PubMed]
24. Wüst, K.; Gervais, A. Do you need a Blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 2018; 45–54. [Google Scholar] [CrossRef]
25. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of Blockchains in the internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutor*, 2019; *21*: 1676–1717. [Google Scholar] [CrossRef]
26. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst, 2018; *88*: 173–190. [Google Scholar] [CrossRef]