

Integration of IoT and Blockchain

Arshiya S Mohammad 1, M Nawaz Brohi 2, Iftikhar Alam Khan 3

Abstract. At present, we are in the world of digital revolution. Use of smartphones and internet accelerated due to the impact of the novel Covid-19 virus. The whole world started to turn digital. The industrialization of Internet of Things (IoT) enables more devices to connect and communicate which leads to many data transfer transactions. The architecture of IoT is centralized. The distributed and decentralized architecture of Blockchain can be used to provide secure and scalable transactions of IoT devices. Blockchain is a distributed ledger technology, which provides secure data transactions that cannot be tampered and altered. In this paper, we provide advantages and challenges of integrating IoT and Blockchain. We also provide different architectures and algorithms proposed by researchers to provide secure data transactions. We shall also shed light on the future research directions of integrating Blockchain and IoT.

Keywords. Integration, Internet of Things, Blockchain, Distributed Ledger, Smart Transportation, Logistics.

1. Introduction

IoT is a recent dominant research area, which leads the world to the digital revolution by providing many applications such as smart home, smart city, smart healthcare, smart agriculture, smart transportation and logistics and many more. IoT in simple words could be defined as network of connected devices (1). The IoT invented by Kevin Ashton in1999. IoT is a network that not only connects people and devices (2). According to statista forecast 2030 the number of IoT devices is almost triple from 8.74 billion in 2020 to more than 25.4 billion IoT devices in 2030 (3).

¹ Senior Lecturer, Department of Creative Computing, Bath Spa University, Academic Centre Ras Al Khaimah, UAE, arshiya@bathspa.ae

² Professor, Department of Creative Computing, Bath Spa University, Academic Centre Ras Al Khaimah, UAE, mnbrohi@bathspa.ae

³ Senior Lecturer, Department of Creative Computing, Bath Spa University, Academic Center Ras Al Khaimah, UAE iftikhar@bathspa.ae



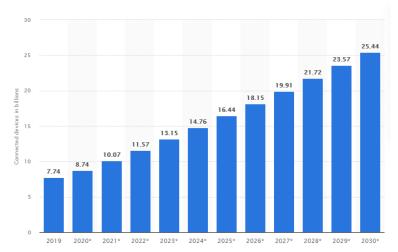


Figure 1: Expected Internet of Things (IoT) connected from 2019 to 2030 (3)

2. IoT Architecture:

The simple IoT architecture consists of three layers as shown in below figure. The major components of IoT architecture are Application layer, Server/Cloud, gateways and devices.

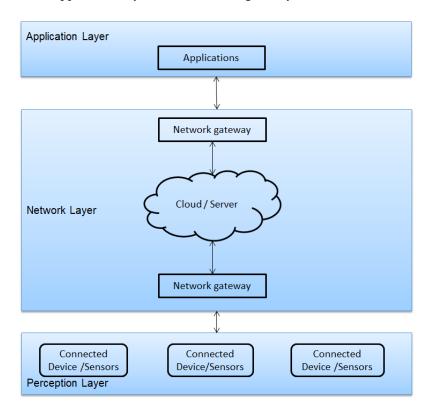


Figure 2: Three layered IoT Architecture

The Perception layer contains the devices sensors also called as physical layer. The devices/sensors collect the data and send it to the network layer. Network layers responsible for connecting perception layer to application layer. Application layer analyse, process the received data,



and provide the requested service by sending the back the service through network layer to the devices in physical layer.

2.1 Challenges of the IoT centralized model

The architecture of IoT is centralized. There are certain challenges of the centralized IoT architecture stated as follows.

Single Point of Failure- If server goes down entire IoT system fails.

Security and privacy - Due to centralized IoT model the data processing and storage is done in single database, which may lead to security issues such as DoS attacks, and the data's privacy and integrity could be challenged.

Scalability - Centralized IoT model works well with limited IoT devices if number of IoT devices increases the network gets complex and scalability issues arises.

Accessibility and Diversity- Heterogeneous IoT devices connected to centralize IoT model causes difficulties to access the network.

Cost - The cost involved to maintain high capability hardware and software of centralized server and database.

3. Block chain

In the world with the Internet of things, a vast set of opportunities can emerge from a block chain. The technology-Block chain allows individuals, small-scale firms, business organizations or any entity to exchange any digital assets in terms of transactions without intermediaries and ensures validity and synchronization of those transactions.

3.1 Structure of Blockchain

A block chain is a tamper-evident, shared digital ledger that records transactions in a public or private peer-to-peer network (4). A distributed ledger is a type of database that is shared, replicated, and synchronized among the members of a decentralized network (4). The digital ledger operates in a distributed network with untrusted nodes. Block chain technology works in a sequential chain of blocks where each block has a list of transactions. These blocks linked to form a chain, a new block added to the recent block, and hence it named as block chain.

Structure of blocks consists of a header and a body section. The header section consists of hash values of previous block and current block and nonce value. The body section consists of data.



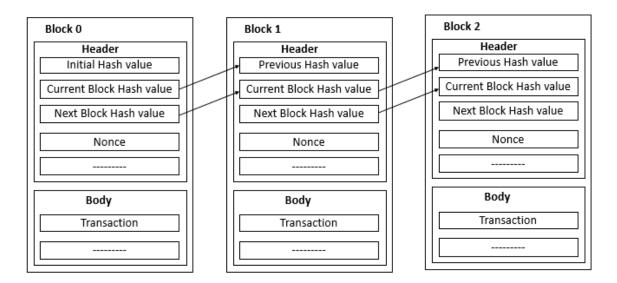


Figure 3: Structure of blocks in Blockchain

Instead of depending on intermediaries or third parties (financial institutions), entities of block chain network use a consensus protocol, cryptographic hashes and digital signatures to perform transactions. Consensus protocol ensures tampered less transactions, cryptographic hash algorithms such as SHA ensures different hash values are generated for different input and digital signatures ensures that the transaction originates from an authorized node.

3.2 Types of Blockchains:

There are two types of block chains. They are public block chain and private block chain.

In a public block chain, any node can join the distributed network to be synchronized with the network each node should solve complex cryptographic problems. Examples of public block chains are Bitcoin and Ethereum.

In private blockchain, to join the network a node needs an invitation or permission and must be validated. Example of a private blockchain is IBM's hyper ledger.

3.3 Lifecycle of transaction in block chain

Lifecycle of transaction in block chain consists of multiple steps. A node in the network initiates the transaction and broadcasted to all other nodes of block chain. The miners then validate and verify the transaction. Once the block mined by the miners, it added to the existing block chain.

3.4 Benefits of Block chain

Block chain technology revolutionizes in many sectors like banking, supply chain, education etc. Benefits of block chain are as follows

Decentralization: Blockchain does not use centralized databases. The transactions of the blockchain are valid and authorized.



Efficiency: No interference from third parties makes the transaction time efficient. Smart contract functionality where an action is triggered automatically when certain criteria in the contract are satisfied. This also reduces time and cost of transaction.

Auditability: As the transactions of blockchain recorded permanently, it makes audit trials available for an asset. Hence makes it easy to authenticate the asset.

Traceability: The lifecycle of the asset easily can be traced in the blockchain. Transfer of ownership can also be done from one person to another in blockchain without using paper.

Security: Use of complex cryptographic algorithms makes the information stored in the blockchain authentic.

Transparency: Blockchain provides transparency regarding the transactions, which reduces work delays and enhances the efficiency of transactions.

3.5 Smart contracts

A smart contract is a collection of code/ functions and data/state that resides at specific address on the blockchain and executes when specific conditions are met (5). Szabo (24) first defined the term smart contract in 1994. Smart contracts can be applied on various applications such as financial transactions, Prediction markets, Internet of Things (IoT) and many more (25). The integration of smart contracts and IoT leads to secure sharing of information and provides automated services to the users.

Despite the bright side of smart contracts, several concerns continue to undermine their adoption, such as security threats, vulnerabilities, and legal issues.

4. Recent researches on Integration of IoT and Blockchain

Blockchain is adopting the latest technologies like AI, IoT, cloud computing and many more. Industries are using the concept of blockchain with the emerging technologies like IoT to enable trust worthy transactions. Billions of devices are connected to IoT. According to cisco, globally, there will be 27.1 billion networked devices in 2021, up from 17.1 billion in 2016. As per (6) the number of interacting devices using the aforementioned communication was forecasted to grow from 780 million connected devices in 2016 to 3.3 billion devices in 2021. Many recent research works shows the integration of IoT and Blockchain and presents the advantages and challenges of integrating IoT with Blockchain.

The research paper (8) states that the personal data of users are secured by combining blockchain with off-blockchain where a user does not need to depend on trusted third parties. The bitcoin blockchain concept is used to provide security of IoT devices using proof of concept protocol (9). The fair access framework proposed in (9) introduces new types of transactions that are used to grant, get, and delegate and revoke access. As per (9) the principles used were User driven and transparency, Fairness using blockchain, distributed architecture and fine-granularity. An OM-AM framework that consists of four layers (Objective, Model, Architecture and Mechanism) is used as a reference model for Fair Access model proposed in (9).

In 2016 USENIX Annual Technical Conference (10), the limitations of Namecoin were presented a new concept of Block stack was introduced. The Block stack is a blockchain-based naming and storage system. Block stack that provides users with a unique human readable user names and public key infrastructure (PKI) based on Namecoin was proposed in (11). Namecoin is a cryptocurrency, which has same features of bitcoin and an additional feature to hold the arbitrary data in the form of name/value



(12). Name coin was to decentralize DNS using Blockchain technology. Later in 2017 a new public key infrastructure – cecoin was developed. This concept is based on distributed ledger and avoids central repository failure of PKI. The previous method is of using PKI where certificate authority issues certificates using the concept of encryption and digital signatures to issue public key of the owners. However, the risk of single point failure exits as the architecture is centralized. To avoid this major failure the cecoin was developed.

In 2017 a multi, layered IoT was developed using blockchian (13). Instead of using the general distributed blockchain in (13) researchers proposed a multi layered blockchain is used which enhances IoT device ability and safety, reduces the loads at the nodes of different layers, provides peer to peer communication between nodes and provides secure and reliable IoT network. (13) Also provides the drawbacks of multi-layered blockchain that are enhancement in the cost of total network, availability time of devices and number of resources.

The decentralized architecture for access control based on the Block chain called as Control Chain was proposed in (14) which does not require third party and provides transparent, fault tolerant, scalable, compatible and secure connections between IoT devices.

IoTChain architecture (15) proposed in 2018 allows secure access and authentication for IoT devices. The researchers proposed their own proof of possession mechanism to perform transactions and store data on block chain using Ethereum platform.

In 2019, researchers proposed a method to increase security of IoT devices and to extend connectivity to other IoT devices using blockchain technology and the Whitelist (16). According to the observations in (16), when applied this stated method to the IoT network simulation environments the number of devices vulnerable to security was reduced by 48.5% compared with traditional IoT environments.

The architecture – BlockIoTIntelligence(17) which combines the concepts of blockchain, IoT and AI, was proposed in 2020. This paper also provides how "Blockchain driven AI reduces the issues of AI using blockchain and also how AI driven Blockchain reduces the issue of blockchain using AI. The researchers in (17) also describes the future directions with BlockIoTIntelligence architecture of converging blockchain and AI to achieve the goal of scalable and secure IoT with cloud intelligence, fog intelligence, edge intelligence and device intelligence.

In (18) the researcher discuss about the IoT and Blockchain-based Framework for Healthcare. Due to the pandemic affect in 2019 caused by Novel corona virus many healthcare systems are working with applications to help out the infected people and to get their health information using the smart devices .This paper also discuss about the different smart app to detect corona virus such as Aarogya Setu, Kwarantanna domowa, Tawakkalna, TraceTogether, LetsBeatCOVID and CovidWatch.

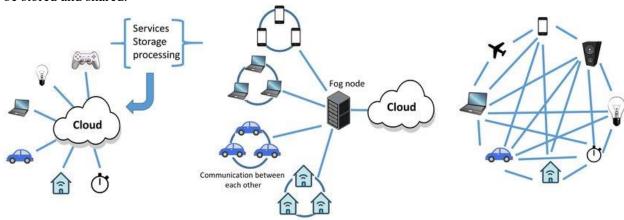
To enhance security of IoT devices connected, research is going on blockchain based encryption algorithms. In 2021, the authors simplified the Directed Acyclic graph based blockchain in (19) and also proposed a new AES –CBC algorithm which periodically changes the private key and IV value. The results of the experiments conducted in(19) on 10 IoT devices connected by DAG based blockchain conclude that the new AES-CBC proposed algorithm reduces the cost and time taken by conventional AES-CBC algorithm by 20%.

In the paper (20) researchers proposed, a hybrid blockchain mechanism based on 5G MEC smart grid using and deployed it on MEC server using public and private blockchian. This mechanism proposed solved the coding and identification problems of massive smart grid IoT devices. The impact of Hybrid blockchain when applied to various blockchain consensus algorithms such as PoW, PoS, DPoS, PDFT was also presented in (20).



5. Integration of Blockchain and IoT

As shown figure 4, there is lot of changes in the current IoT Architecture but it is still dependent on the traditional centralized system. In the future there is possibility to use decentralized architecture to connect IoT devices (6). This may lead to form the peer to peer wireless sensor network, where each device shall have sensors and all devices would be connected and data collected from these devices shall be stored and shared.



Past IoT Architecture Present IoT Architecture Future IoT Architecture

Figure 4: Architecture of IoT in the past, present and future (6).

Security and Privacy of the data shared is most important aspects that is to be focused in this digital revolution caused by IoT. The concept of Cloud computing that provides access to data and eliminates the presence of hardware devices is one of the major reasons for the new digital revolution. Even though the security is provided by this centralized system of cloud computing but many security vulnerabilities still exits. As per (7) the first IoT Botnet was discovered at Proofpoint the security firm in December 2013. The DDos attacks are the most frequent attacks in the IoT connected devices. The hackers can easily hack the system if the IoT devices are unsecure and can launch the DDos attacks (21)

The other issue of IoT devices is scalability. The centralized IoT system becomes congested when more devices are connected in the network and the services provided like authentication, connection of different devices, availability would be time consuming.

5.1 IoT-Blockchain architecture

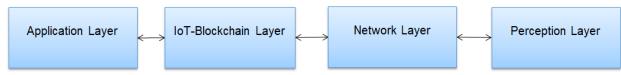


Figure 6: IoT-Blockchain Architecture

The IoT Blockchain architecture is represented in above diagram. The new layer IoT-Blockchian layer is added to the traditional IoT architecture. This layer integrates the features of Blockchain to IoT.



5.2 Challenges of security and scalability of IoT solved by Blockchain

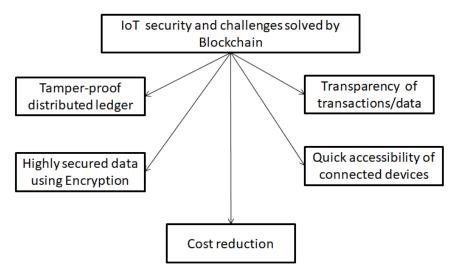


Figure 5: Challenges of security and scalability of IoT solved by Blockchain

The issues of security and scalability of the IoT could be addressed by Blockchain technology and is represented in above figure 2. Blockchain uses the concept of distributed ledgers, which are tamper proofs, and hence eliminates the need of trust among the devices connected. IoT data can be stored securely using the high-level encryption techniques used by Blockchain. Transparency of data is provided by the concept of blockchain where any authorized device can access the current data and the previous data. The connectivity and accessibility of devices could be enhanced by using Blockchain. The overhead costs of IoT devices caused by connectivity protocols are reduced.

5.3 Challenges of IoT with Blockchain

In this section, we shall discuss the some of the challenges of integrating IoT and Blockchain. The technology of Blockchain was developed considering high performance devices, which require huge hardware and software capabilities to provide secure, tamper-proof transactions. Whereas some of the IoT devices are very small and huge amount of data is processed in the IoT network. Integrating IoT with Blockchain is challenging. A few challenges are listed below.

Storage- the transactions of small data works well Blockchain concept but the IoT devices generate huge data, integrating these two concepts is still challenging. The storage capacity is among the major issues of blockchain, as the total size of Bitcoin and Ethereum blockchains are around 150 and 400 gigabytes respectively. However, IoT devices generate data in Zettabytes. Therefore, Blockchain is not suitable for storing IoT data (22)

Huge data stored by IoT devices could be reduced by storing only the required data for analysis/knowledge extraction. In addition, the bandwidth of the transactions of Blockchain concept could be increases to support IoT data.

Data security - The data collected from IoT devices has a major security issues due to the some of its features like mobility/ wireless network. The Blockchain concept could be used to reduce the security issues. However, it would be difficult to maintain the integrity of data before applying the Blockchain to the IoT data; in this case, Blockchain provides security to already tampered data, which would be of no use. Before integrating IoT with Blockchain, it is important to check the integrity of data collected by IoT devices.



Scalability- One of the major issues of integrating IoT with blockchain is scalability. The Blockchian works well with small-scale network as the throughput (transactions/second) of Blockchain network is low compared to the large-scale IoT network. As per (23) the throughput of Bitcoin is seven transactions/second. In addition, Ethereum can process 20 transactions/second. However, the IoT network for example PayPal has throughput of 170 and VISA has 2000 as it throughput. One solution to issue could be developing more scalable consensus algorithm to increase throughput of Blockchain network.

Availability of Resources- Most of the IoT devices connected have less storage and less processing power. The Blockchain network requires high processing power. The issue of resources required to integrate the IoT with Blockchain could be resolved using the concept of cloud computing with IoT and Blockchain.

6. Conclusion

In this present digital revolution era, the demand of IoT is extremely high. The major challenges of IoT arise due to the centralized architecture of IoT such as scalability and security can be resolved using the decentralized architecture of Blockchain. The distributed ledger concept of Blockchain eliminates the issues of single point failure, provides tamper-proof transactions, and efficient data security. Both the IoT and Blockchain when integrated provide a better solution for above-mentioned issues. This paper presents basics of IoT and Blockchain and describes how integration of IoT and Blockchain eliminates the issues caused due to the centralized model of IoT. This paper also provides some of the recent studies on integration of IoT and Blockchain. Some of challenges of integrating IoT and Blockchain follow this. Some of the future research directions are presented at the end.

References

- [1] ethereum.org. 2021. *Introduction to smart contracts* | *ethereum.org*. [online] Available at: https://ethereum.org/en/developers/docs/smart-contracts/ [Accessed 7 September 2021].
- [2] Statista. 2021. *Topic: Internet of Things (IoT)*. [online] Available at: https://www.statista.com/topics/2637/internet-of-things/ [Accessed 7 September 2021].
- [3] Statista. 2021. *Topic: Internet of Things (IoT)*. [online] Available at: https://www.statista.com/topics/2637/internet-of-things/ [Accessed 7 September 2021].
- [4] Brakeville, S. and Perepa, B., 2018. *Blockchain Basics: Introduction to Distributed Ledgers*. [online] IBM Developer. Available at: https://developer.ibm.com/tutorials/cl-blockchain-basics-intro-bluemix-trs/ [Accessed 7 September 2021].
- [5] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in IEEE Access, vol. 9, pp. 28177-28193, 2021, doi: 10.1109/ACCESS.2021.3052867.
- [6] Nartey, C., Tchao, E., Gadze, J., Keelson, E., Klogo, G., Kommey, B. and Diawuo, K., 2021. On Blockchain and IoT Integration Platforms: Current Implementation Challenges and Future Perspectives. *Wireless Communications and Mobile Computing*, 2021, pp.1-25, Article ID 6672482.
- [7] Stergiou, C., Psannis, K., Kim, B. and Gupta, B., 2018. Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems*, 78, pp.964-975.
- [8] Zyskind, G., Nathan, O. and Pentland, A., 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops,.
- [9] Ouaddah, A., Abou Elkalam, A. and Ait Ouahman, A., 2016. FairAccess: a new Blockchain-



- based access control framework for the Internet of Things. *Security and Communication Networks*, 9(18), pp.5943-5964.
- [10] Ali, M., Nelson, J., Shea, R. and J. Freedman, M., 2016. Blockstack: A Global Naming and Storage System Secured by Blockchains. In: 2016 USENIX Annual Technical Conference (USENIX ATC '16). [online] USENIX. Available at:

 https://www.usenix.org/conference/atc16/technical-sessions/presentation/ali [Accessed 7 September 2021].
- [11] Pavithran, D. and Shaalan, K., 2019. Towards Creating Public Key Authentication for IoT Blockchain. 2019 Sixth HCT Information Technology Trends (ITT),.
- [12] Kalodner, H., Carlsten, M., Ellenbogen, P., Bonneau, J. and Narayanan, A., n.d. *An empirical study of Namecoin and lessons for decentralized namespace design*. [online] Cs.princeton.edu. Available at: https://www.cs.princeton.edu/~arvindn/publications/namespaces.pdf [Accessed 8 September 2021].
- [13] Li, C. and Zhang, L., 2017. A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things. 2017 IEEE International Congress on Internet of Things (ICIOT),.
- [14] Pinno, O., Gregio, A. and De Bona, L., 2017. ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. *GLOBECOM 2017 2017 IEEE Global Communications Conference*.
- [15] Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., Rousseau, F., Tourancheau, B., Veltri, L. and Zanichelli, F., 2018. IoTChain: A blockchain security architecture for the Internet of Things. 2018 IEEE Wireless Communications and Networking Conference (WCNC),.
- [16] Choi, Y., Kang, H. and Lee, I., 2019. Scalable and Secure Internet of Things Connectivity. *Electronics*, 8(7), p.752.
- [17] Singh, S., Rathore, S. and Park, J., 2020. BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. *Future Generation Computer Systems*, 110, pp.721-743.
- [18] Alam, T., 2020. Internet of Things and Blockchain-Based Framework for Coronavirus (COVID-19) Disease. *SSRN Electronic Journal*.
- [19] Lee, S. and Sim, K., 2021. Design and Hardware Implementation of a Simplified DAG-Based Blockchain and New AES-CBC Algorithm for IoT Security. *Electronics*, 10(9), p.1127.
- [20] Wang, D., Wang, H. and Fu, Y., 2021. Blockchain-based IoT device identification and management in 5G smart grid. *EURASIP Journal on Wireless Communications and Networking*, 2021(1).
- [21] Deloitte Switzerland. 2021. Can blockchain accelerate Internet of Things (IoT) adoption | Deloitte Switzerland. [online] Available at: https://www2.deloitte.com/ch/en/pages/innovation/articles/blockchain-accelerate-iot-adoption.html [Accessed 8 September 2021].
- [22] Atlam, H., Azad, M., Alzahrani, A. and Wills, G., 2020. A Review of Blockchain in Internet of Things and AI. *Big Data and Cognitive Computing*, 4(4), p.28.
- [23] Samaniego, M., Jamsrandorj, U. and Deters, R., 2016. Blockchain as a Service for IoT. 2016 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),.
- [24] Szabo, N., 1996. Smart Contracts: Building Blocks for Digital Markets. [online] Fon.hum.uva.nl. Available at: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smartcontracts2.html [Accessed 8 July 2021].
- [25] Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R. and Wang, F., 2018. An Overview of Smart Contract: Architecture, Applications, and Future Trends. 2018 IEEE Intelligent Vehicles Symposium (IV),.